Privacy Requirements

Scope

Each Department must continue to operate within its legal authority and restrictions with regard to the collection, use, disclosure and retention of personally identifiable information (PII). Where the statutes governing PII are more restrictive, they will control. However, if there is no agency, program or subject matter specific law governing the PII, the more general law will apply.

This report is intended to review laws that impact the Enterprise. Necessarily, there will be privacy laws not covered in this report, as they impact isolated agencies. If a privacy law is not covered in the report, but may have a wide impact, a request should be made to the Executive Branch Privacy Office for inclusion in the next report. This report will be reviewed and updated on an annual basis, with issuance in the fall of each year.

Laws are divided into two categories – Federal and State. Each law is identified by common name, legal citation with a description, implications and electronic source. Each law is mapped to applicable Privacy Principles.

Federal

1.1. Privacy Act of 1974, Section 7
5 U.S.C. § 552a (note)

Description:

Except in certain situations, federal, state and local government cannot deny an individual "any right, benefit, or privilege provided by law because of such individual's refusal to disclose his Social Security account number." This prohibition does not apply in two scenarios. The first is where a federal law mandates disclosure of the SSN. The second is where a federal, state or local agency "maintain[s] a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual."

Where government requests an individual to disclose his or her SSN, the Department must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it."

While enforcement is not specifically delineated in the law, private individuals have successfully sued state and local government in the 4th Circuit, and other circuits, under this law.

Implications:

- Departments must assess where they collect the SSN and tie it to a right, benefit or privilege, where they are mandated by federal law to do so and where they have a system of records, required by statute or regulation, in existence before January 1, 1975.
- Where Departments cannot collect the SSN under the Privacy Act, they must assess their business operations and implement an alternative method of identifying individuals.
- Where Departments can continue to collect the SSN under the Privacy Act, they must provide notice consistent with this law.
- Where Departments collect the SSN lawfully, they must not use it for any secondary purpose that does not meet the Privacy Act requirements and is not delineated in the Notice.
- Departments must adopt policies and procedures regarding SSN collection and use, and display of the Privacy Act notice.

Source:

http://www4.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-notes.html (See note on "Disclosure of Social Security Number")
CRS Report-SSN Laws
http://www.justice.gov/opcl/1974ssnu.htm

Principles:

Notice, Minimum Necessary and Limited Use

1.2. Tax Reform Act of 1976
42 U.S.C. § 405(c) (2)

Description:

This law amends the Social Security Act by authorizing states to use the SSN as an identifier in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law and allows states to require individuals to furnish their SSN to the state with regard to these programs.

Note: Congress has passed additional laws over the years allowing states to use the SSN as an identifier in a variety of programs. *See* CRS Report-SSN Laws

Implications:

- Use of the SSN as an identifier in certain instances is authorized by federal law.
- As Departments develop their notices, and determine from a business process standpoint that they must use the SSN as an identifier, they must identify the federal law which gives them the authority to do so. This law may provide the requisite authority for the SSN collection.

Source:

http://www4.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00000405----000-.html

Principles:

Notice, Minimum Necessary and Limited Use

1.3. Omnibus Reconciliation Act of 1990, § 2201(c)
42 U.S.C. § 405(c) (2) (C) (viii) (I).

Description:

This law requires that all SSNs and related records obtained by federal or state authorized persons pursuant to laws enacted on or after October 1, 1990 "shall be confidential, and no authorized person shall disclose any such Social Security account number or related record."

Because West Virginia law requires that all state executive branch agencies safeguard all SSNs and treat them as confidential, with disclosure as authorized by law, W. Va. Code § 5A-8-21, 22, the only additional requirement yielded by this federal statute is with regard to the prohibition on disclosure.

The Attorney General of Oregon has interpreted this prohibition on disclosure to simply mean that there can be no unauthorized redisclosure. 47 Or. Op. Atty. Gen. 1, 37, 1993 WL 602063 (Or. A.G. 1993). An authorized redisclosure includes a redisclosure with the individual's informed consent. Therefore, if an individual who receives a legally sufficient Privacy Act Notice discloses his or her SSN to the Department and thereby consents to the uses and disclosures identified in the notice, the Department may redisclose the SSN per the Notice. *Id*.

Unauthorized willful disclosures of SSNs and related records are felonies and punishable by fines and/or imprisonment.

Implications:

- Departments shall assess where they are disclosing SSNs.
- Departments shall adopt policies and procedures ensuring that they only disclose SSNs in accordance with their legally sufficient Notices.
- Departments shall safeguard SSNs and keep them confidential.

Source:

http://www4.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00000405----000-.html

Principles:

Consent , Minimum Necessary and Limited Use, Security Safeguards

1.3.1 Federal Tax Return Information
IRC §§ 6103(p)(4), 7213 and 7213A
IRS Publication 1075

Description:

The Internal Revenue Code (IRC) makes information pertaining to a taxpayer's identity and tax return information confidential. Criminal penalties are imposed for the unauthorized disclosure of federal income tax returns or federal return information. Additionally, the unauthorized inspection of federal tax returns or return information is a crime. These crimes are felonies or misdemeanors depending upon the crime committed and upon conviction the person may be fined or imprisoned or both fined and imprisoned.

The Commissioner of Internal Revenue is authorized to enter into exchange of information agreements with state revenue department. Those departments and their employees are subject to the same confidentiality requirements for federal tax returns and return information as are imposed on the Internal Revenue Service and its employees.

Additionally, contractors with either the Internal Revenue Service or a state revenue agency that have access to federal returns and return information in order to perform the contracts are subject to the same confidentiality rules and criminal provisions applicable to employees of the Internal Revenue Service or the state revenue agency

Implication

Departments that have federal tax return information provided by the Internal Revenue Service must preserve the confidentiality of that information and ensure that there is no unauthorized disclosure of that information

Source:

http://www.law.cornell.edu/uscode/text/26/6103
http://www.law.cornell.edu/uscode/text/26/7213
http://www.law.cornell.edu/uscode/text/26/7213A
http://www.irs.gov/pub/irs-pdf/p1075.pdf

Principles:

Minimum necessary and limited use, Security Safeguards

1.4. Health Insurance Portability and Accountability Act, (HIPAA), "Privacy Rule"
45 C.F.R. §§ 160 and 164

Description:

The HIPAA Privacy Rule became effective April 14, 2003 and applies to health plans, health care providers who conduct covered health transactions electronically (including submitting claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which the Department of Health and Human Services ("HHS") has established standards under the HIPAA Transactions Rule), and health care clearinghouses. This Rule provides a foundation of federal protections for the privacy of protected health information ("PHI") in any medium including electronic records, paper records and verbal communications. The Rule does not replace State law that grants individuals even greater privacy protections. The Rule covers: uses and disclosures of PHI, authorizations, minimum necessary use and disclosure, workforce policies, patients' rights, organizational matters, legal matters, and safeguards.

The HIPAA Privacy Rule regulations detail requirements for HIPAA Privacy Notices provided by covered entities that maintain a website that provides information about the Covered Entity's customer services or benefits. In such instances, privacy practices must be prominently posted on the website and a link to the full privacy notice must be available through the website. The Office for Civil Rights enforces the Privacy Rule. There are civil and criminal penalties for noncompliance.

HIPAA was amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"). Subtitle D of the Act amends HIPAA privacy and security rules. The development of health information technology (electronic health records, personal health records, health information exchanges) has resulted in additional risks; HITECH builds on HIPAA's privacy and security rules to address these new risks.

HITECH extends certain HIPAA requirements to Business Associates. This means that the HIPAA requirements, formerly imposed on Business Associates only through contracts with Covered Entities, are now directly applied to Business Associates by law. However, these requirements must also be included in contracts between Covered Entities and Business Associates. Business Associates are now subject to HIPAA security requirements for administrative, physical, and technical information safeguards, as well as most HIPAA privacy requirements. In addition, Business Associates are required to detect and report security breaches to Covered Entities. Finally, Business Associates are subject to civil and criminal penalties if they violate these requirements.

Covered Entities must comply with an individual's request to restrict the disclosure of PHI if the disclosure is to a health plan for payment or health care operations, and if the PHI pertains solely to a health care item or service that has already been paid in full, out of pocket by the individual.

In situations where the "minimum necessary" standard applies, Covered Entities must limit the disclosure of PHI to, if possible, a Limited Data Set, or if not practicable, to the

minimum necessary to accomplish the intended purpose of the disclosure. The Covered Entity or Business Associate disclosing the PHI must determine what information is minimally necessary to meet the need.

If a Covered Entity uses or maintains electronic health records ("EHR"), individuals are entitled, upon request, to an accounting of disclosures for treatment, payment, and health care operations that occurred during the three (3) years prior to the request. A Covered Entity may respond to an individual's accounting request in one of two ways: (1) provide an accounting of all disclosures made by the Covered Entity and its Business Associates or (2) provide a list of the Covered Entity's disclosures and a list of all Business Associates. Business Associates must then supply a list of disclosures upon request from the individual.

A Covered Entity or a Business Associate may not sell EHR or PHI without authorization from the individual unless (1) the information is to be used for public health activities, research or treatment; (2) there is a sale, transfer, merger or consolidation of all or part of the covered entity with another covered entity; (3) the price covers the Business Associate's cost to produce the information at the request of the Covered Entity; or (4) the price covers the cost to provide the individual with a copy of his or her PHI.

If a Covered Entity uses or maintains EHR, individuals have a right to obtain their PHI in electronic format ("e-PHI"). An individual can also designate a third party recipient of e-PHI. Fees may not exceed the cost of labor to process the request.

The HITECH Act adds a breach notification provision to HIPAA; it requires Covered Entities to notify each affected individual, generally by first class mail, when it discovers that PHI that is not encrypted or otherwise made indecipherable has been breached. A breach occurs when unsecured PHI has been or is reasonably believed to have been accessed, acquired or disclosed as a result of such breach, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. Business Associates that discover a breach must notify the Covered Entity of each individual whose unsecured information was placed at risk as a result of the breach. There is no requirement of actual harm in order to trigger notification. A breach is considered to be discovered as of the first day the breach is known to the Business Associate or Covered Entity. All required notifications must be made without unreasonable delay and in no case later than sixty (60) calendar days after the discovery of the breach by the covered entity or business associate.

The definition of a breach, the content of the notice and method of delivery contained in HITECH are similar to comparable provisions in West Virginia's breach notification law. However, HITECH requires covered entities to provide notice to prominent media outlets within the State or jurisdiction if a breach of unsecured PHI affects or is reasonably believed to affect more than five hundred (500) State residents. HITECH also requires that notice be provided to the Secretary of HHS in the case of breaches involving more than five hundred (500) individuals. HIPAA requires covered entities to

mitigate the potentially harmful effects of improper disclosures but there is no express obligation to notify affected individuals. The breach notification obligations are also imposed on personal health record vendors, even if they are not Covered Entities under HIPAA.

The regulations provide that a Covered Entity must "identify and respond to suspected or known security incidents; mitigate to the extent practicable, harmful effects of security incidents known to the Covered Entity and document security incidents and their outcomes." 45 C.F.R. § 164.308(a)(6)(ii).

Vendors of personal health records (PHR) and other entities not covered under HIPAA are also subject to certain notification requirements if there is a breach of unsecured PHR-identifiable health information that is maintained or offered by the vendor. After a vendor discovers a breach, the vendor must (1) notify the individuals whose unsecured PHR-identifiable health information was acquired by an unauthorized person as a result of the breach and (2) notify the Federal Trade Commission ("FTC"). The FTC must notify the Secretary of any such breach. *See* Section 1.5 for further discussion on FTC's Health Breach Notification Rule.

HITECH requires the Secretary to formally investigate if a preliminary investigation of the facts of a complaint indicate the possibility that the violation was a result of willful neglect. If willful neglect is found to have occurred, the Secretary must impose mandatory penalties. HITECH also increases the civil penalties for willful neglect. These penalties can extend up to $250,000, with repeat or uncorrected violations extending up to $1.5 million. Additionally, HITECH authorizes the State Attorney General to bring a civil action on behalf of state residents, as *parens patriae*, to enjoin violations and to obtain damages and attorney fees.

Note:

Numerous lawsuits were filed challenging the Patient Protection and Affordable Care Act of 2010 ("PPACA"). On November 4, 2011, the Supreme Court granted a petition for writ of certiorari and oral arguments regarding PPACA, including the individual health insurance mandate, were heard March 26 – 28, 2012. The HITECH Act could possibly be limited or affected by this challenge to the constitutionality of PPACA. However, on June 28, 3012, the Supreme Court upheld the constitutionality of PPACA. *National Federation of Independent Business v Sebelius*, 567 U.S. ___ (2012).

On March 24, 2012, the Office of Management and Budget ("OMB") accepted for review the final HITECH Regulations from HHS. OMB has ninety (90) days to complete its review, and it is anticipated that the final regulations will be published in July, 2012 or thereafter. The regulations will finalize: (1) the 2010 HITECH proposed rule, (2) the 2009 interim final rule regarding breach notification, (3) the 2009 interim final rule regarding enforcement and (4) the 2009 proposed rule under the Genetic Information Nondiscrimination Act.

Implications:

- Departments have completed their HIPAA assessment and implementation and are in the compliance phase. If any Department has not completed its assessment, please contact the State Privacy Office.
- Any Department that undertakes a new health-related responsibility should complete a HIPAA Covered Entity Assessment.
- HIPAA covered agencies must ensure that they have policies, procedures and Business Associate Agreements to carry out the Privacy Rule's requirements and that they have trained their workforce as appropriate.
- Business Associates will be subject to HIPAA security and privacy provisions, as well as sanctions for violation of Business Associate requirements. Business Associates agreements will need to be modified to reflect these changes. See Section 4.0, West Virginia HIPAA Addendum.
- Consumers must be notified of data security breaches involving "unsecured" PHI. Both Covered Entities and Business Associates must comply with these notice requirements, although the latter's notification obligation runs to the Covered Entity. See Section 1.4.2.
- Vendors of personal health records and their service providers are now subject to the security breach notification requirement.
- Individuals may prohibit Covered Entities from disclosing certain self-pay services to health plans.
- Limited data sets are the new default for PHI disclosures governed by the minimum necessary standard.
- Covered entities using EHRs must include all disclosures of PHI for treatment, payment, and health operations in the past three (3) years when an individual requests an accounting.
- Upon request, covered entities must provide an individual with PHI in electronic form and transmit it to designated third parties.
- HIPAA covered agencies should review the HIPAA Privacy Rule requirements and its amendments needed to engage in compliance activities to ensure that the HIPAA Privacy Rule provisions are met and updated.
- Business Associates must keep a HIPAA-compliant log of certain disclosures of PHI for each individual's PHI, which includes disclosures resulting from a breach.
- Departments will continue to monitor new regulations implementing the statutory amendments under HITECH, including the Notice of Proposed Rulemaking pertaining to Modifications to the HIPAA Privacy, Security and Enforcement Rules issued in the Federal Register on July 14, 2010. This proposed new rule is entitled "Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act." The proposed rule (1) expands individuals' rights to access their information and to restrict certain types of disclosures of protected health information to health plans; (2) requires business associates of HIPAA-covered entities to be under most of the same rules as the covered entities; (3) sets new limitations on the use and disclosure of protected health information for marketing and fundraising; and (4) prohibits the sale of protected health information without patient authorization. Another Proposed Rulemaking was issued May 31, 2011 and is

entitled “HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act.” This proposed rule concerns the requirement for the accounting of disclosures under the HIPAA. The proposed rule would give individuals the right to obtain a report identifying all those who have electronically accessed their protected health information.

Source:

http://www.hhs.gov/ocr/hipaa/finalreg.html
http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html
http://www.hhs.gov/ocr/hipaa/
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
http://www.access.gpo.gov/nara/cfr/waisidx_02/45cfr160_02.html
http://www.access.gpo.gov/nara/cfr/waisidx_04/45cfr164_04.html
http://edocket.access.gpo.gov/2010/pdf/2010-16718.pdf
http://www.gpo.gov/fdsys/pkg/FR-2011-05-31/pdf/2011-13297.pdf

Principles:

Accountability, Notice, Minimum Necessary and Limited Use, Consent, Individual Rights, Security Safeguards

1.4.1. Health Insurance Portability and Accountability Act (HIPAA), "Security Rule" 45 C.F.R. § 164.302 -§ 164.318

Description:

The HIPAA Security Rule, published by the Department of Health and Human Services (HHS), describes what "Covered Entities" *must* do to make sure patients' medical files are secure. The Security Rule is in effect for all entities. The HITECH Act amends the Security Rule and makes certain portions of the Rule directly applicable to Business Associates of a Covered Entity; the additional requirements must be set forth in the Business Associate Agreement.

The Security Rule is important to patients because, like the Privacy Rule, it creates a national standard for protecting the confidentiality, integrity and availability of e-PHI. This means that all health care providers, health plans and health care clearinghouses that transmit information electronically must adopt a data security plan.

Only health information maintained or transmitted in electronic format is covered by the Security Rule; thus, paper records stored in filing cabinets are not subject to the security standards. For example, e-PHI includes telephone voice response and fax back systems because these systems may be used as input and output devices for electronic systems but does not include paper-to-paper faxes, video teleconferencing or messages left on voicemail because the information being exchanged did not exist in electronic format prior to transmission.

The Security Rule, according to the HHS, is designed to be flexible, establishing a security framework. All covered entities must have a written security plan. The HHS identifies three components as necessary for the security plan. These are:

- Administrative safeguards
- Physical safeguards
- Technical safeguards

Each of the three major categories has a number of additional subcategories. In addition to the required components, other factors are "addressable" items that should be considered and adopted if suitable to the Covered Entity's size and organization. Among the addressable factors set forth in the Security Rule as part of rule compliance is continuing education. This includes periodic security updates. The continuing evaluation process should be developed and implemented to maintain sustainability of HIPAA Security compliance. Systematic and controlled reviews of changes that affect data security are necessary for a comprehensive evaluation program. Each Department must identify, train and assign individuals to key processes associated with technology and operations change.

Entities are required under the Security Rule to conduct risk analyses to implement the required security standards. On July 14, 2010, the United States Department of Health and Human Services, Office of Civil Rights ("OCR"), issued a "Final Guidance on Risk

Analysis" designed to assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. The Guidance sets forth these sample questions for identify issues an organization may wish to consider in implementing the Security Rule:

• Have you identified the e-PHI within your organization? This includes e-PHI that you create, receive, maintain or transmit.
• What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain or transmit e-PHI?
• What are the human, natural, and environmental threats to information systems that contain e-PHI?

The Guidance contains additional discussion of steps to assess and safeguard e-PHI. The Security Rule requires covered entities to adopt "incident" reporting procedures. According to HHS, the Security Rule does not specifically require any incident reporting to outside entities. Thus, the HIPAA Security Rule does not require breach notification.

Implications:

- Ensure the confidentiality, integrity, and availability of all e-PHI that the Covered Entity creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of e-PHI.
- Protect against any reasonably anticipated uses or disclosures of e-PHI that are prohibited by the HIPAA Privacy Rule.
- Ensure compliance by the workforce.
- Develop methods and procedures for continuing evaluation to maintain sustainability of HIPAA Security compliance.
- Establish procedures for periodic evaluation of implemented security measures.
- HIPAA covered entities should notify their business associates of the security rule, notification and enforcement penalty changes as a result of the HITECH Act.
- HIPAA covered entities should develop a plan to revise their business associate agreements to reflect the changes. See Section 4.0, Agency HIPAA Business Associate Addendum.
- Enforcement of HIPAA security provisions will be stricter with the possibility of larger civil penalties and State Attorney General enforcement.

Note:

Pursuant to the Code of Federal Regulations establishing Conditions for Federal Financial Participation, 45 CFR § 95.621, Departments are responsible for the security of all automated data processing systems involved in the administration of HHS programs, and includes the establishment of a security plan that outlines how software and data security will be maintained. This section further requires that Departments conduct a review and evaluation of physical and data security operating procedures and

personnel practices on a biennial basis. CMS issued a letter to state Medicaid directors dated September 20, 2006, which specifically requires state agencies and their Business Associates to comply with the HIPAA Security requirements. In addition, CMS is requiring that all contracts include a provision requiring contractors to report to the state Medicaid staff breaches of privacy or security. The state is then obligated to report the breach to CMS.

Implications/Best Practices:

- Departments must remember that risk mitigation is the compliance objective.
- Security plans should present Department security features/requirements in terms of their risk mitigation benefits.
- Department security plans should document the risk mitigation rationale and effectiveness.
- Departments must balance the cost-effective dollar arguments against the higher obligation to ensure patient privacy and safety.
- Develop procedures to keep privacy and security concerns coupled.
- Departments who receive federal funding should check with their federal funder for additional requirements.
- Departments with HIPAA Business Associates must evaluate and confirm compliance with the Security Rule as Business Associates are now subject to HIPAA's (increased) civil and criminal penalties.

Source:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

Principles:

Security Safeguards, Notice, Accountability

1.4.2. Breach Notification for Unsecured Protected Health Information, Interim Final Rules

45 C.F.R. Parts 160 & 164; 74 F.R. 42740

Description:

The Interim Final Rule for Breach Notification became effective on September 23, 2009. These "breach notification" regulations implement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA). The regulations require health care providers, health plans, and other entities covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to notify individuals when their health information is breached.

The regulations, developed by OCR, require health care providers and other Covered Entities to promptly notify affected individuals of a Breach, as well as the HHS Secretary and the media in cases where a Breach affects more than five hundred (500) individuals. Breaches affecting fewer than five hundred (500) individuals will be reported to the HHS Secretary on an annual basis. The regulations also require Business Associates of Covered Entities to notify the Covered Entity of breaches at or by the Business Associate.

The new requirements apply if all of the following are present:

- There is a "breach." The Rule defines "breach" to mean (subject to exceptions discussed below) the unauthorized acquisition, access, use or disclosure of PHI.
- The PHI is "unsecured." The Rule defines "unsecured protected health information" to mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS guidance.
- The breach "compromises the security of the PHI." Under the Rule, this occurs when there is a significant risk of financial, reputational, or other harm to the individual whose PHI has been compromised.

Note:

The Federal Trade Commission (FTC) issued companion breach notification requirements for vendors of personal health records (PHRs) and their third party service providers following the discovery of a breach of unsecured PHR-identifiable health information. For further discussion *see* Section 1.5. Entities operating as Covered Entities and Business Associates are not subject to the FTC breach notification rules. But in certain instances where a breach involves an entity providing PHRs to customers of a Covered Entity through a business associate arrangement, and directly to the public, the FTC will deem compliance with the HHS Rule as compliance with its own breach notification rules.

HHS has emphasized that this Rule does not modify a Covered Entity's responsibilities with respect to the HIPAA Security Rule nor does it impose any new requirements upon Covered Entities to encrypt all PHI. A Covered Entity may still be in compliance with the Security Rule even if it decides not to encrypt electronic PHI so long as it utilizes another method to safeguard information in compliance with the Security Rule. However, if such method is not in compliance with the requirements of the Rule with respect to securing PHI, then the Covered Entity will be required to provide a breach notification to affected individuals upon a breach of unsecured PHI. The Rule preempts contrary State breach notification laws. A Covered Entity must still comply with requirements of State law which are in addition to the requirements of the Rule, but not contrary to such requirements (such as additional elements required to be included in a notice). *See* Section 3.18, West Virginia Breach Notification Law.

On July 28, 2010, the Department of Health and Human Services offered a "Breach Notification Final Rule Update" which states in its entirety as follows:

> The Interim Final Rule for Breach Notification for Unsecured Protected Health Information, issued pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act, was published in the Federal Register on August 24, 2009, and became effective on September 23, 2009. During the 60-day public comment period on the Interim Final Rule, HHS received approximately 120 comments.
>
> HHS reviewed the public comment on the interim rule and developed a final rule, which was submitted to the Office of Management and Budget (OMB) for Executive Order 12866 regulatory review on May 14, 2010. At this time, however, HHS is withdrawing the breach notification final rule from OMB review to allow for further consideration, given the Department's experience to date in administering the regulations. This is a complex issue and the Administration is committed to ensuring that individuals' health information is secured to the extent possible to avoid unauthorized uses and disclosures, and that individuals are appropriately notified when incidents do occur. We intend to publish a final rule in the Federal Register in the coming months.
>
> Until such time as a new final rule is issued, the Interim Final Rule that became effective on September 23, 2009, remains in effect.

Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 Title XIII (HITECH Act) of the American Recovery and Reinvestment Act of 2009

On April 19, 2009, HHS issued "Guidance" on technologies that protect health information. To determine when information is "unsecured" and notification is required by the HHS and FTC rules, the guidance specifies encryption and destruction technologies and methodologies that render protected health information unusable, unreadable or indecipherable to unauthorized individuals, and therefore "secured". Entities subject to the HHS and FTC regulations that secure health information as specified by the guidance through encryption or destruction are relieved from having to notify in the event of a breach of such information. This guidance will be updated annually.

According to the Guidance, PHI is rendered unusable, unreasonable or indecipherable to unauthorized individuals only if one or more of the following methods are used:

(1) *Encryption*. Electronic PHI is only secured where it has been encrypted. The HIPAA Security Rule specifies encryption to mean the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. The Rule identifies the various encryption processes which are judged to meet this standard. Such confidential process or key that might enable decryption must not have been breached. To avoid a breach of the confidential process or key, decryption tools should be kept on a separate device or at a location separate from the data they are used to encrypt or decrypt.

(2) *Destruction*. Hard copy PHI, such as paper or film media, is only secured when it has been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.

Note:

As noted above, final regulations regarding breach notification are anticipated to be issued in July, 2012 or thereafter.

Implications:

- Departments will assess and determine the types of information they maintain that must be "secured" and will evaluate whether the use of encryption technology is appropriate.
- Departments will develop and implement destruction policies pertaining to media containing PHI.
- Develop policies and procedures for determining whether a breach has occurred. Issues to cover include:

- Steps for identifying a potential breach incident.
- Steps for determining whether the incident is an impermissible use or disclosure of PHI under the HIPAA Privacy Rule.
- Steps for performing a risk assessment analysis to determine the level of harm that the breach has caused to any individuals.
- Steps to ensure that affected individuals, the media and/or HHS receive proper notification, as required.
- Documentation for each step of these processes.
- Discussion of the new policies and procedures with the employer's HIPAA privacy officer, who will be responsible for this additional enforcement.

- Departments will work with each Business Associate regarding implementation of policies and procedures relating to breach notification. Issues to cover include:
  - Requesting a copy of the security breach notification policies and procedures that the business associate will implement.
  - Discussing the reporting of reportable and non-reportable breaches.
  - Determining the role of the business associate in identifying breaches and suspected breaches related to the business associate's service agreement.
  - Allocating responsibility for fulfilling the notification requirements when a reportable breach has occurred and maintaining any related data required under the interim final rule.
  - Amending the indemnification provisions of the business associate agreement to ensure that the appropriate party bears the costs associated with the notification requirements and liability for failure to comply with them.

Source:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf

Principles:
Notice

1.4.3 Affordable Insurance Exchanges
45 CFR Parts 155, 156 and 157

Description:

The Patient Protection and Affordable Care Act of 2010 as amended by the Health Care and Education Reconciliation Act of 2010, collectively known as the Affordable Care Act ("ACA"), provides for states to create affordable insurance exchanges to provide competitive marketplaces for individuals and small business employers to directly compare available private health insurance options on the basis of price, quality and other factors. Some have questioned whether or not and to what extent these new exchanges will be subject to the Privacy Act and the HIPAA Security Rule previously discussed a 1.4.1.

On March 27, 2012, the Department of Health and Human Services published a final rule implementing the affordable insurance exchange provisions and requirements of the ACA. This rule took effect May 29, 2012. Section 155.260 of this rule provides for the privacy and protection of personally identifiable information collected by an exchange. Key aspects of this rule include, but are not limited to:

Where the exchange creates or collects personally identifiable information for the purpose of determining eligibility for enrollment in a qualified health plan; determining eligibility for other insurance affordability programs; or determining exemptions from the individual health insurance mandate, the exchange may only use or disclose the personally identifiable information necessary to carry out its functions as described in Section 155.200 of the rule.

The exchange may not create, collect, use or disclose personally identifiable information while the exchange is fulfilling its responsibilities under Section 155.200 unless the creation, collection, use or disclosure are consistent with Section 155.260.

The exchange must establish and implement privacy and security standards that are consistent Section 155.260.

For purposes of implementing the security safeguards required by Section 155.260, the exchange must establish and implement certain operational, technical, administrative and physical safeguards that are consistent with Section 155.260 and any other applicable law.

Implications:

The West Virginia Health Insurance Exchange will be subject to the requirements of this new federal regulation.

Source:

http://www.healthreformgps.org/wp-content/uploads/2012-6125.pdf

Principles:

Confidentiality, security and limited use of personally identifiable information

1.5. Federal Trade Commission's Health Breach Notification Rule
16 C.F.R. Part 318

Description:

The HITECH Act requires the FTC to implement and enforce breach notification provisions that apply to vendors of personal health records and their third-party service providers.

The FTC breach notification rule applies if you are:

- A vendor of personal health records (PHRs);
- A PHR-related entity; or
- A third-party service provider for a vendor of PHRs or a PHR-related entity.

Covered Entities and Business Associates are not subject to the FTC's breach notification rule but must comply with the HHS's breach notification rule.

Notice must be given when there is an "unauthorized acquisition" of "PHR-identifiable health information" that is "unsecured" and in a "personal health record". The definitions of these terms are defined in the Rule and the definitions of the terms are important.

If there is a security breach and you are a "vendor of personal health records" or a "PHR-related entity", the Rule provides the next steps that should be taken. The subject entity must notify:

1. each affected person who is a citizen or resident of the United States;
2. the Federal Trade Commission; and
3. in some cases, the media.

The rule sets forth who to notify, when to notify them, how to notify them and what information to include.

Persons: If a vendor of personal health records or a PHR-related entity experiences a breach of unsecured personal health information, each affected person should receive notice "without unreasonable delay" and within sixty (60) calendar days after the breach is discovered. The sixty (60) day period begins to run the day the breach becomes known to someone in the company [vendor of PHRs or PHR-related entity] or the day someone reasonably should have known about it. Those subject to the Rule must act without unreasonable delay. This means if a company discovers the breach and gathers the necessary information within thirty (30) days, it is unreasonable to wait until the 60th day to notify the people whose information was breached.

FTC: The Rule requires notice to the FTC. The timing depends on the number of people affected by the breach.

500 or more people: The FTC must receive notice as soon as possible and within ten (10) days after discovering the breach. The report should be provided on the FTC's form at: www.ftc.gov/healthbreach.

Fewer than 500 people: Notice must be given, but more time is given to provide the information. The FTC form noted above must be provided with forms documenting any other breaches during the same calendar year involving fewer than five hundred (500) people within sixty (60) calendar days following the end of the calendar year.

The Media: When at least five hundred (500) residents of a particular state, District of Columbia or U.S. Territory or possession are affected by a breach, notice must be provided to prominent media outlets serving the relevant locale, including Internet media where appropriate, without unreasonable delay and within sixty (60) calendar days after the breach is discovered. This notice is in addition to individual notices.

Third-party service providers to a vendor of PHR or a PHR-related entity also have notice requirements under the Rule. If the third-party service provider experiences a breach, it must notify an official designated in its contract with the vendor or a senior official within the vendor company—without unreasonable delay and with sixty (60) calendar days of discovering the breach. The Rule requires the third-party provider to identify for the vendor client each person whose information may be involved in the breach. The third-party service provider must receive an acknowledgement from the vendor client that they received the notice.

Personal notice must be provided by first-class mail to the individual at the last known address of the individual, or by e-mail, if the individual receives a clear, conspicuous opportunity to receive notification by first-class mail and does not exercise that choice. In the case of a deceased individual, notice must be provided to the next of kin, if the contact information is provided along with authorization to contact them.

Substitute notice is required if the contact information for ten (10) or more individuals is insufficient or out-of-date. Substitute notice is accomplished by:

1. a clear and conspicuous posting for ninety (90) days on your home page; or
2. a notice in major print or broadcast media where those people likely live.

The content of the notice should include the following:

- a brief description of what happened, including the date (if known) and the date you discovered the breach;
- the kind of PHR-identifiable health information involved in the breach. For example, insurance information, social security numbers, financial account data, dates of birth, medication information, etc.;
- Steps individuals should take to protect themselves from potential harm resulting from the breach;

- A brief description of what the entity that suffered the breach is doing to investigate the breach, to mitigate harm, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll free telephone number, and e-mail address, web site or postal address.

The FTC will treat each violation of the Rule as an unfair or deceptive act or practice in violation of a Federal Trade Commission regulation. Businesses that violate the Rule may be subject to a civil penalty of up to $16,000 per violation

Note:

The FTC's Rule preempts contradictory state breach notification laws, but not those that impose additional – but non-contradictory – breach notification requirements. For example, West Virginia's breach notification law requires breach notices to include advice on monitoring credit reports or contact information for consumer reporting agencies. While these content requirements are different from the FTC Rule's requirements, they are not contradictory. In this example, you could comply with both federal and West Virginia requirements by including all the information in a single breach notice. The FTC Rule does not require you to send multiple breach notices to comply with both state and federal law.

The HITECH Act could possibly be limited or affected by one of more of the numerous ongoing lawsuits challenging the constitutionality of one of the law's provisions. The potential impact on the portions of the HITECH Act involving HIPAA are uncertain, and these cases should be monitored.

Implications:

- Departments should identify a "team" to handle breach and related notifications
- The "team" members might include the following: chief information officer, compliance officer, human resources, legal/risk management, public relations with input from State Chief Privacy Officer
- Departments should develop templates of policies and procedures and forms of documents compliant with the new federal standard and applicable state law breach notification requirements
- Development of an action plan, including checklists of key contacts such as media and others both within and outside the Department, will enable Departments to effectively and timely respond to potential breach notification situations.

Source:

http://www.ftc.gov/os/2009/08/R911002hbn.pdf
http://business.ftc.gov/documents/bus56-complying-ftcs-health-breach-notification-rule

Principles:

Notice

1.6. Confidentiality of Substance Abuse Records, Reports of Violations
42 U.S.C. § 290dd-2; 42 C.F.R. Part 2, *et seq*.

Description:

Substance abuse records created in connection with federally assisted treatment programs are confidential. Federal assistance includes programs conducted by a federal agency; licensed, certified, registered or otherwise authorized by a federal agency; funded by a federal agency; and assisted by the IRS through allowance of income tax deductions or through the granting of tax exempt status to the program. Confidential information includes name, address, social security number, fingerprints, photograph or similar information by which the identity of the patient can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information. The protections begin when a person applies for or has been given a diagnosis or treatment for alcohol or substance abuse at a federally assisted program; protections are extended to former and deceased patients. Use and disclosure must be limited to the minimum necessary. Disclosure may not occur without patient consent, unless an exception applies, and restrictions apply to recipients of the information. One significant exception is alcohol and drug testing that is not conducted as part of a diagnosis of or treatment for an alcohol or other substance problem is not protected by these confidentiality rules. The regulations specify the elements that must be in the consent and the required accompanying statement. The regulations also require security, notice of privacy rights to patients, patient access and restriction on use.

A violation of the regulations may be reported to the U.S. Attorney in the judicial district in which the violation occurs. A methadone program which is believed to have violated the regulations may be reported to the Regional Offices of the Food and Drug Administration.

There are criminal penalties for violation of these regulations.

Note:

The Substance Abuse & Mental Health Services Administration (SAMHSA) and the Office of the National Coordinator (ONC) for Health Information Technology have posted Frequently Asked Questions (FAQs) for Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE). The FAQs outline the general provisions of 42 C.F.R. Part 2, provide guidance on its application to electronic health records, and identify methods for including substance abuse patient record information into health information exchange that is consistent with the Federal statute. The FAQs are not meant to provide legal advice.

Implications:

- Departments should determine whether they receive and/or create substance abuse patient records from a federally assisted facility.
- Departments that do receive and/or create substance abuse patient records must adopt policies and procedures to ensure compliance with these regulations.

- The CPO shall forward the information regarding the security requirements to the Director of Information Security.
- Departments cannot apply W.Va. Code § 27-3-1(b) (6) as revised by H.B. 3184, effective June 08, 2007, to substance abuse records from federally assisted programs.

Departments should review the issued guidance applying the Substance Abuse Confidentiality Regulations to health information exchange and assess whether any policies or procedures should be updated.

Source:

http://www4.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00000290--dd002-.html
http://www.access.gpo.gov/nara/cfr/waisidx_03/42cfr2_03.html
http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=addc04a3ac00116c60239752b5bae03d&rgn=div8&view=text&node=42:1.0.1.1.2.1.1.5&idno=42
http://www.samhsa.gov/HealthPrivacy/
http://www.samhsa.gov/healthprivacy/docs/ehr-faqs.pdf

Principles:

Notice, Minimum Necessary and Limited Use, Consent, Individual Rights, Security Safeguards

1.7. Gramm-Leach Bliley-Act (GLB)
15 U.S.C. § 6801, 16 C.F.R. § 313; 72 F.R. 62890

Description:

Any financial institution that provides financial products or services to consumers must comply with the GLB privacy provisions. An entity has consumers if it provides financial products or services to individuals, not businesses, to be used primarily for their personal, family, or household purposes. Under the Federal Trade Commission's (FTC) Privacy Rule, a financial institution means "any institution the business of which is engaging in financial activities as described in § 4(k) of the Bank Holding Company Act of 1956 [12 U.S.C. § 1843(k)]." *See* 16 C.F.R. § 313.3(k) (1). Further, you are not a financial institution unless you are *significantly engaged* in financial activities. *Id.* State entities do not fall under the definition of a "financial institution" under GLB.

Financial activities generally include lending money, investing for others, insuring against loss, providing financial advice, making a market in securities, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, non-bank lenders, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors, and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors. Government entities that provide financial products such as student loans or mortgages are financial institutions that engage in financial activities. However, before GLB applies, the financial institution must be "significantly engaged" in financial activities, which is a flexible standard that takes into account all the facts and circumstances.

GLB provides privacy, safeguarding and pretexting (regarding obtaining information under false pretenses) requirements. GLB privacy protections require initial and annual distribution of privacy notices and place limits on disclosures of nonpublic personal information. The FTC is authorized to enforce this law.

The Financial Services Regulatory Relief Act of 2006 amended the GLB to require certain federal agencies to propose a succinct and comprehensible model form that allows consumers to easily compare the privacy practices of different financial institutions, and has an easy-to-read font.

Effective on January 1, 2011, financial institutions that wish to be protected under the FTC's "safe harbor" must convert to a new model privacy notice. The "safe harbor" provides the financial institutions with security in that they are assured that the notice satisfies the disclosure requirements for notices. To retain protection, the financial institution should not amend the FTC's model notice, including, without limitation, its wording or formatting. Failure to adopt the model notice does not mean that the notice is deficient but merely that it does not enjoy automatic protection. Likewise the prior "model clauses" no longer enjoy "safe harbor" protection as of December 31, 2011. Financial institutions should examine their notices and policies and consider updating to the new model privacy notice. Eight federal regulators released a model consumer

privacy notice online form builder to assist financial institutions in preparing acceptable forms.

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (the "Act") amended several sections of GLB. Most rulemaking authority under the Act was transferred to the new Consumer Financial Protection Bureau (the "CFPB") except that the CFPB will not have authority to establish financial institutions data safeguards – this remains with the FTC. Additionally, the SEC and the FTC are charged with the power to prescribe certain GLB rules for entities under their jurisdictions. Enforcement of the regulations will reside with the CFPB for banks over 10 billion in assets, then with the FTC or other functional regulators. Residual jurisdiction will be the FTC and the CFPB. These changes became effective on July 21, 2011.

On December 21, 2011, as a consequence of the CFPB gaining authority over GLB, the CFPB published for comment a new proposed Regulation P. There were no substantive changes to the Regulation.

Implications/Best Practices:

None. State entities do not fall under the definition of "financial institution" under GLB. Nevertheless, as a matter of creating policies for "best practices," it may be useful to consider the following implications that apply to "financial institutions":

- Entities must assess whether they are significantly engaged in financial activities.
- If applicable, financial institutions must develop policies and procedures to ensure an initial and annual notice is distributed and that there are limits on disclosure of nonpublic personal information.
- Financial institutions may rely on the Model Privacy Form as a safe harbor to provide disclosures under the GLB privacy rule.
- The CPO shall forward the information regarding the safeguard requirements to the Director of Information Security.

Source:

http://www4.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00006801----000-.html
http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html
http://ftc.gov/privacy/privacyinitiatives/PrivacyModelForm.pdf
http://www.sec.gov/rules/final/2009/34-61003_modelprivacyform_nooptout.pdf
http://www.federalreserve.gov/bankinforeg/privacy_notice_instructions.pdf

Principles:

Notice, Consent, Minimum Necessary and Limited Use, Security Safeguards

1.7.1. Gramm-Leach-Bliley Act (GLB), “Safeguards Rule”
15 U.S.C. § 6801-09; 16 C.F.R. § 314

Description:

The Safeguards Rule, which implements the security requirements of the GLB, requires financial institutions to have reasonable written policies and procedures to ensure the integrity and confidentiality of customer information. State entities do not fall under the definition of a “financial institution” under GLB.

The Rule is intended to be flexible to accommodate the wide range of entities covered by GLB, as well as the wide range of circumstances entities face in securing customer information. Accordingly, the Rule requires financial institutions to implement a written information security program that is appropriate to the entity's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its program, each financial institution must also: (1) assign one or more employees to oversee the program; (2) conduct a risk assessment; (3) put safeguards in place to control the risks identified in the assessment and regularly test and monitor them; (4) require service providers, by written contract, to protect customers' personal information; and, (5) periodically update its security program.

GLB regulations require entities to prepare a written information security plan that describes an entity’s program to protect client information. All programs must be appropriate to the size and complexity, the nature and scope of activities, and the sensitivity of the client information at issue.

Entities significantly engaged in financial activities must:

1. Designate the employee or employees to coordinate the safeguards.
2. Identify and assess the risks to customer information in each relevant area of an entity’s operation, and evaluate the effectiveness of current safeguards for controlling these risks.
3. Design a safeguards program and detail the plans to regularly monitor it and then do so.
4. Select appropriate service providers and require them (by contract) to implement the safeguards, and oversee them.
5. Evaluate the program and explain adjustments in light of changes to an entity’s business arrangements or the results of security tests or monitoring.

The Act states that the Safeguards Rule remains with the prudential banking regulator, which could include the CFPB for appropriately qualifying financial institutions, and with the FTC.

Implications/Best Practices:

None. State entities do not fall under the definition of "financial institution" under GLB. Nevertheless, as a matter of creating policies for "best practices," it may be useful to consider the following implications that apply to "financial institutions":

Financial institutions should:

- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems.
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.
- Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

Additionally, financial institutions should develop a written information security system, a written response program and develop procedures for:

- Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information breaches have occurred.
- Notifying its primary Federal regulator (if applicable) as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information.
- Immediately notifying law enforcement in situations involving likely criminal violations requiring immediate attention.
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access, such as by monitoring, freezing, or closing affected accounts, while preserving records and other evidence.
- Disposing of customer information in a secure manner and where applicable, consistent with the FTC's Disposal Rule.
- Developing policies for employees who telecommute or those who store or access customer information from their personal computers or mobile devices.

Source:

http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html
http://www.ftc.gov/os/2002/05/67fr36585.pdf
http://www.ftc.gov/privacy/glbact/glboutline.pdf
http://business.ftc.gov/documents/alt152-disposing-consumer-report-information-new-rule-tells-how

Principles:

Accountability, Security Safeguards, Notice

1.8. Fair Credit Reporting Act as amended (FCRA) (including the Fair and Accurate Credit Transactions Act of 2003 (FACT Act))
15 U.S.C. § 1681 *et seq*., (Pub. L. 108-159, 111 Stat. 1952); 16 C.F.R. § 682; 72 Fed. Reg. 63718 *et seq*. (Nov. 9, 2007)

Description:

FCRA governs a consumer reporting agency's creation and disclosure of consumer reports. A consumer reporting agency is "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." This summary will not address the consumer reporting agency's responsibilities or the responsibilities of furnishers of information to consumer reporting agencies.

Entities procuring consumer reports must comply with FCRA. A consumer report concerns a "consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" and may be used for credit, insurance, employment or other business decision making. In the employment context, notice must be given that a consumer report will be procured and authorization obtained. Before an adverse action is taken, the person intending to take the action must provide the consumer with notice, a copy of the report, including the disclosure of the person's credit score and related information and a description of their rights. In an employee misconduct investigation conducted by a third party, notice does not need to be given to the employee and no authorization is required. At the end of the investigation, the employee is only entitled to a notice of adverse action and a summary of the report. Consumer reports may only be used for authorized purposes; however, a consumer's identifying information may be given to a governmental agency without regard to the purpose. Before an entity procures an investigative consumer report, which is a report based upon personal interviews with neighbors, friends or associates, it must give notice to the consumer and certify compliance to the consumer reporting agency. FCRA generally requires that consumers be given notice and an opportunity to opt-out with respect to marketing from organizations affiliated with the original receiver of the consumer report.

FCRA also governs truncation of credit card and debit card numbers. Beginning December 4, 2006, any machines in use before January 1, 2005 that print receipts for credit card or debit card transactions shall not print more than the last 5 digits of the card number or the expiration date. For all other machines put into use on or after January 1, 2005, this requirement went into effect December 4, 2004.

The Act also impacted FCRA and FACT Act. Primary rulemaking authority was transferred to the CFPB, which impacted prior interpretations and commentary on FCRA. On July 26, 2011, the FTC rescinded its Statements of General Policy or Interpretation ("Commentary") under the FCRA, which were initially issued in 1990. The FTC stated that the Commentary was "obsolete" and "stale" due to its age and the

number of revisions and amendments to FCRA since 1990. Since the "Commentary" was rescinded, it was not transferred to the CFPB and is no longer guiding or relevant in interpreting FCRA.

Enforcement actions may now be brought by the FTC, SEC and the CFPB. There are civil and criminal penalties.

The CFPB is specifically excluded from jurisdiction over consumer reports that are not used in connection with the offering of consumer financial products or services, such as used for tenant screening, employment, et al.

Changes related the CFPB became effective on July 21, 2011.

On February 7, 2012, the FTC warned marketers of 6 mobile background screening apps that they may be in violation of FCRA. The letter states "If you believe your background reports are being used for FCRA or other FCRA purposes, you and your customers who are using your reports for such purposes must comply with FCRA…"

On May 3, 2012, the FTC, the CFPB, and the Department of Justice filed a memorandum of brief supporting the constitutionality of FCRA in Shamara T. King v. General Information Services Inc. (GIS). GIS is arguing that FCRA is an unconstitutional restriction of free speech citing the recent Supreme Court decision in Sorrell v. IMS Health Inc. 131 S. Ct. 2653 (2011).

Note:

The FACT Act adds several new sections to FCRA, primarily of interest to banking institutions and consumer reporting agencies but also potentially pertinent to any entity that maintains consumer information or is a creditor. Regulations have now been issued which provide further compliance details. The FACT Act amends FCRA by requiring that any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose to properly dispose of any such information or compilation. One purpose of the FACT Act is to reduce the risk of consumer fraud and related harms, including identity theft, created by improper disposal of consumer information.

Any business regardless of industry that obtains a consumer report or information derived from a consumer report will be subject to the record disposal rule imposed by the FACT Act. This includes entities that possess or maintain consumer information for a business purpose such as landlords, government agencies, utility companies, telecommunication companies, employers and other users of consumer reports.

Any person that maintains or possesses consumer information is required to take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. Entities covered by the FACT Act will need to consider the sensitivity of the consumer information, the nature and size of the entity operations, the costs and benefits of different disposal methods, and relevant

technological changes. The FTC considers "reasonable measures" to include establishment of policies and procedures for disposal, as well as proper employee training.

Numerous provisions of FACT Act significantly limit the State's ability to regulate much of FCRA's subject matter, as amended.

Like most of the other consumer oriented federal laws, the CFPB will be responsible for issuing rules under the FACT Act.

See Section 1.8.1 for a detailed discussion on the Red Flag Rules.

Implications:

- Departments shall assess where they procure consumer reports.
- Division of Personnel and State Departments, as appropriate, shall adopt policies and procedures to ensure that consumer reports are properly procured and properly destroyed.
- The Chief Privacy Officer shall forward the information regarding the FACTA disposal requirements to the Director of Information Security.
- Division of Purchasing and Departments shall adopt policies and procedures to ensure that all machines purchased that print credit card and debit card receipts shall not print more than the last 5 digits of the card or the expiration date.
- Departments shall periodically assess whether they are subject to the Red Flag Rules.
- Departments that are subject to the Red Flag rules will develop written programs to detect, prevent and mitigate identity theft in connection with covered accounts.

Sources:

http://www.consumerfinance.gov/guidance/supervision/manual/fcra-narrative/
http://www.ftc.gov/os/statutes/031224fcra.pdf

Principles:

Notice, Consent, Minimum Necessary and Limited Use, Security Safeguards

1.8.1 Identity Theft “Red Flags” Rule
16 C.F.R. § 681.1

Description:

The Identity Theft “Red Flags” Rule requires “creditors” and “financial institutions” to develop written plans to prevent and detect identity theft. “Creditors” and “financial institutions” are broadly defined in the Rule. The Dodd-Frank Act added swap dealers and major swap participants to those entities that must comply with identity red flag rules and guidelines. The Rule is a section of the Fair and Accurate Credit Transactions Act (FACT Act) of 2003, a federal law which requires the establishment of guidelines for financial institutions and creditors regarding identity theft. The Red Flags Rule sets out how certain businesses and organizations must develop, implement, and administer their own Identity theft prevention programs. Each program must include four basic elements, which together create a framework to address the threat of identity theft:

1) Each program must include reasonable policies and procedures to identify the “red flags” of identity theft that may occur in the day-to-day operation of a business. Red flags are suspicious patterns or practices, or specific activities, that indicate the possibility of identity theft. For example, if a customer has to provide some form of identification to open an account, an ID that looks fake would be a “red flag.”

2) Each program must be designed to detect the red flags previously identified. For example, if a fake ID is identified as a red flag, there must be procedures in place to detect possible fake, forged, or altered identification.

3) Each program must spell out appropriate actions to take when red flags have been detected.

4) Because identity theft is an ever-changing threat, each program must address periodical re-evaluations of the red-flag program procedures.

The Rule is in effect and enforcement began on January 1, 2011.

The Red Flag Program and Clarification Act of 2010 was signed by President Obama on December 18, 2010. The Clarification Act amended the definition of a “creditor” covered by the Red Flags Rules to creditors who in the ordinary course of their business, (i) obtain or use consumer reports, directly or indirectly, in connection with the transaction; (ii) furnish information to consumer reporting agencies, in connection with a credit transaction; or (iii) advance funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person. It then limited the definition of creditors to exclude those “that advance funds on behalf of a person for expenses incidental to a service provided to that individual.” This exclusion was meant to refute the FTC’s position that the Red Flag Rules were applicable to attorneys and medical providers, including hospitals,

nursing homes and clinics. However, if any of those excluded entities obtain or use consumer reports or report to consumer reporting agencies, then the Red Flags rule are applicable to those entities.

On February 28, 2012, the Securities and Exchange Commission and the Commodity Futures Trading Commission proposed new Red Flags rules and guidelines pursuant to the requirements of Title X of the Dodd-Frank Act. The provisions set forth rules requiring the entities under these two commissions jurisdictions 1) to address identity theft by requiring financial institutions and creditors to develop and implement a written identity theft prevention program to detect, prevent and mitigate identity theft in connection with existing or the opening of new accounts; and 2) to establish special requirements for any credit and debit card issuers that are subject to the commissions' jurisdictions to assess their rules. Generally, these new rules do not contain new requirements from the FTC rules, nor do they expand the scope of those rules. Comments to the proposed regulations were due as of May 7, 2012.

Implications

- Departments shall periodically assess whether they are subject to the Red Flags Rule.
- Departments shall identify red flags for its own type of covered accounts and incorporate them into the Department's identity theft program.
- Departments that are subject to the Red Flags Rule will develop written programs to detect, prevent and mitigate identity theft in connection with covered accounts.
- Departments may want to consider incorporating the FTC's "illustrative examples" to the extent applicable into its identity theft program.
- Hospitals and medical providers should examine their usage of credit reports or their reporting to credit agencies so as to be or remain excluded from the Red Flags rules.

Sources:

www.ftc.gov/redflagsrule
http://www.redflagrules.net/uploads/Red_Flag-Federal_Register.pdf

Principles:

Notice, Consent, Minimum Necessary and Limited Use, Security Safeguards

1.9. Family Educational Rights and Privacy Act of 1974 (FERPA)
20 U.S.C. § 1232g; 34 C.F.R. Part 99 (amended effective January 3, 2012)

Description:

FERPA protects the privacy of student education records and applies to any public or private agency or institution (may be referred to as school) that receives funds under an applicable program of the U.S. Department of Education. Education records are those records, files, documents, and other materials which contain information directly related to a student and are maintained by an educational agency or institution. There are a number of exempted categories of records.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school; parents must be granted access within 45 days after the request is made. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record to a third-party. The authorization form may be paper or electronic. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions:
    - School officials with legitimate educational interest;
    - Other schools to which a student is transferring;
    - Specified officials for audit or evaluation purposes;
    - Appropriate parties in connection with financial aid to a student;
    - Organizations conducting certain studies for or on behalf of the school;
    - Accrediting organizations;
    - To comply with a judicial order or lawfully issued subpoena;
    - Appropriate officials in cases of health and safety emergencies; and,
    - State and local authorities, within a juvenile justice system, pursuant to specific state law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and

dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them.

Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

Failure to comply with FERPA can result in loss of funds from any of the U.S. Department of Education's applicable programs.

The United States Department of Education proposed seven amendments to 34 C.F.R. Part 99 that were published in the Federal Register on April 8, 2011 (Vol. 76, No. 68). Final regulations were filed in the Federal Register on December 2, 2011 (Vol. 76, No. 232). The regulations took effect January 3, 2012..

Implications:

- Departments must assess whether they collect or maintain student education records and receive funds under an applicable program of the U.S. Department of Education to determine FERPA coverage.
- If FERPA applies, Departments shall adopt policies and procedures to ensure that the various requirements are in place.

Source:
http://www4.law.cornell.edu/uscode/html/uscode20/usc_sec_20_00001232---g000-.html

Principles:
Notice, Consent, Individual Rights

1.10. Driver's Privacy Protection Act
18 U.S.C. § 2721

Description:

The Driver's Privacy Protection Act (DPPA) is similar to West Virginia's Uniform Motor Vehicle Records Disclosure Act and restricts public disclosure of personal information contained in DMV records. Personal information includes: photograph, SSN, DLN, name, address, telephone number and medical or disability information. DPPA applies to state DMVs and recipients of personal information from the DMV. The Act permits the release of information to recipients who are using it for one or more specific statutory purposes, or where the subject of the record was furnished an opportunity to limit the release of the information and did not do so. The Act penalizes the procurement of information from motor vehicle records for an unlawful purpose, or the making of a false representation to obtain such information from a DMV.

There are civil and criminal penalties for violation of this law. Additionally, there is a private right of action.

Implications:

- DMV must have policies and procedures to ensure that personal information obtained in connection with the motor vehicle record is only used and disclosed as authorized by law or with the consent of the individual.
- Departments must assess whether they obtain personal information from DMV.
- Departments obtaining personal information from DMV must ensure that they have policies and procedures detailing the use and disclosure of the personal information, as well as the record keeping requirements.

Source:

http://www4.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_123.html

Principles:

Consent, Minimum Necessary and Limited Use, Security Safeguards

1.11. Telephone Consumer Protection Act, Telemarketing Sales Rules
47 U.S.C. § 227, 16 C.F.R. Part 310

Description:

The Act requires entities who use the telephone to solicit individuals, to provide such individuals with the ability to prevent future telephone solicitations. Those who engage in telephone solicitations must maintain and honor lists of individuals who request not to receive such solicitations for ten years. The Act prohibits unsolicited commercial telephone calls using an artificial or pre-recorded voice without consumer consent. Also prohibits the sending of unsolicited advertisements to facsimile machines.

The sales rules regulate telemarketing with regard to deceptive and abusive telemarketing acts or practices. Significantly, this rule establishes the Federal Trade Commission's (FTC) Do-Not-Call list.

The FTC has jurisdiction to enforce this rule against the private sector. The Federal Communications Commission (FCC) (with regard to interstate and international communications), State attorneys general, as well as private citizens, may bring actions under these provisions against state government. State telemarketing laws are not preempted. *See* the discussion regarding Consumer Credit and Protection Act, Telemarketing W. Va. Code § 46A-6F-601.

The FCC approved changes to its telemarketing rule on February 15, 2012, to further protect consumers from unwanted autodialed or prerecorded telephone calls often referred to as "robocalls." These new rules were filed in the Federal Register on June 11, 2012 and take effect July 11, 2012. They:

- Require telemarketers to obtain prior express written consent from consumers, including by electronic means such as a website form, before placing a robocall to a consumer;
- Eliminate the "established business relationship" exemption to the requirement that telemarketing robocalls to residential wireline phones occur only with the prior express consent from the consumer;
- Require telemarketers to provide an automated, interactive "opt-out" mechanism during each robocall so that the consumer can immediately tell the telemarketer to stop calling; and
- Strictly limit the number of abandoned or "dead air" calls that telemarketers can make within each calling campaign.

Implications:

- Departments shall assess whether they engage in telemarketing.
- Departments that engage in telemarketing shall adopt policies and procedures to ensure compliance with this rule and W. Va. Code § 46A-6F-601.

Source:

http://www.ftc.gov/os/2003/01/tsrfrn.pdf
http://www.fcc.gov/guides/robocalls

http://www.gpo.gov/fdsys/pkg/FR-2012-06-11/pdf/2012-13862.pdf
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=46a&art=6F&section=601#06F

Principles:
Notice, Consent, Minimum Necessary and Limited Use, Security Safeguards

Note:
There are special marketing rules which do not neatly fit within the defined principles.

1.12. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, (CAN-SPAM Act)
15 U.S.C. § 7701

Description:
The CAN-SPAM Act establishes requirements for those who send commercial e-mail, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask e-mailers to stop spamming them.

The law covers e-mail whose primary purpose is advertising or promoting a commercial product or service, including content on a Website. The main provisions include: ban on false or misleading header information (e-mail's "From," "To," and routing information – including the originating domain name and e-mail address – must be accurate and identify the person who initiated the e-mail); prohibition on deceptive subject lines; the e-mail must give recipients an opt-out method (the sender has 10 business days to stop sending e-mail to the requestor's e-mail address); and, commercial e-mail must be identified as an advertisement and include the sender's valid physical postal address.

The Federal Trade Commission (FTC) is authorized to enforce the CAN-SPAM Act against the private sector. CAN-SPAM also gives the Department of Justice the authority to enforce its criminal sanctions. Other federal and state agencies, such as the Attorney General, can enforce the law against organizations under their jurisdiction. Companies that provide Internet access may sue violators, as well.

Implications:
- Departments must assess whether they are sending commercial e-mail to advertise a product or service.
- Departments transmitting commercial e-mail to advertise or promote a product or service shall adopt policies and procedures to ensure compliance with this law.

Sources:
http://www.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00007701----000-.html
www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm

Principles:
Notice, Consent

1.13. Junk Fax Prevention Act of 2005
47 U.S.C. § 227(b) (1) (C)

Description:
This law amends the Communications Act of 1934 to prohibit a person from using any telephone facsimile (fax) machine, computer, or other device to send, to another fax machine, an unsolicited advertisement to a person who has requested that such sender not send such advertisements, or to any other person unless: (1) the sender has an established business relationship with the person; (2) the sender obtained the fax number through voluntary communication from the recipient or from an Internet directory or site to which the recipient voluntarily made the fax number available for public distribution; and (3) the advertisement contains a conspicuous notice on its first page that the recipient may request not to be sent any further unsolicited advertisements, and includes a domestic telephone and fax number (neither of which can be a pay-per-call number) for sending such a request.

Additionally, the Federal Communications Commission (FCC) has issued rules regarding faxing advertisements; the fax must identify sender on either the top or bottom margin of each page with telephone number and the date and time the fax is sent.

The FCC (with regard to interstate and international communications) and the West Virginia Attorney General may enforce this law. There are civil and criminal penalties. Additionally, there is a private right of action.

Implications:
- Departments must assess whether they advertise by fax.
- Departments which advertise via fax shall ensure that they adopt policies and procedures in compliance with this law.

Sources:
Junk Fax Prevention Act of 2005

Principles:
Notice, Consent

1.14. Children's On-line Privacy Protection Act (COPPA)
15 U.S.C. § 6501 *et seq*., 16 C.F.R. Part 312

Description:

The Children's Online Privacy Protection Act (COPPA), which took effect in April of 2000, prohibits certain unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personal information from children on the Internet pursuant to COPPA's requirements. The Federal Trade Commission (FTC) issued the Children's Online Privacy Protection Rule (the COPPA Rule) which imposes requirements on website or online services directed to children under 13 years of age or that have actual knowledge that it collects personal information from children under 13 years of age. This includes websites that allow children to use interactive communication tools. So, even if the site is not collecting information about children, if a child's personal information can be made public on the site (such as through a message board), there may be COPPA liability.

Websites cannot require a child to provide personal information as a condition of participating when it is not necessary to do so.

The FTC oversees the implementation of this law. Its website provides extensive information on COPPA. With certain exceptions, COPPA is to be enforced by the FTC under the FTC Act. The FTC may enforce the state's compliance with COPPA or those acting under color of state law pursuant to the enforcement provisions of COPPA, which incorporate by reference the means, jurisdiction, powers and duties of the FTC Act. Although such an instance may be rare, it is important for websites and online service providers to be cognizant of their online activities.

The State Attorney General may bring an action as *parens patriae,* if he/she has reason to believe that an interest of the residents of West Virginia has been or is threatened or adversely affected by the engagement of any person in a practice that violates any regulation of COPPA. The Attorney General may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction. Suits may be brought to achieve compliance with the Act, as well as to recover monetary damages.

In September, 2011, the FTC filed in the Federal Register (Vol. 76, No 187) proposed changes in 16 C.F.R. Part 312 that are intended to respond to changes in online technology and to streamline the rule. The FTC proposed to modify certain definitions in the rule and to update the requirements set forth in the notice, parental consent, confidentiality and security, and safe harbor provisions. Additionally, the FTC proposed adding a new provision covering data retention and deletion. The public comment period closed November 28, 2011. The final rule has not been published in the Federal Register, as of this date.

Implications:

COPPA requires that websites and online services directed to children under age 13 must:

- Post a clearly written privacy policy with links to the notice provided on the home page and at each area where the site or online service collects personal information from children.
- Describe the kinds of information collected from children, i.e. name, address, e-mail, hobbies, age (this applies to all information, not just personal information).
- Explain how the information is collected, whether directly from the child and/or behind the scenes through cookies.
- Explain how the website operator uses the personal information (i.e. marketing to children, notifying contest members, etc.), and whether it is disclosed to third parties.
- Provide parents with contact information, address, phone number, and e-mail address, for all operators collecting or maintaining children's personal information.
- Obtain parental consent before collecting, using, or disclosing personal information about a child.
- Provide parents with the ability to review, correct, and delete information about their children collected by such services.
- Maintain reasonable procedures "to protect the confidentiality, security, and integrity of personal information collected from children."

Source:

http://www.ftc.gov/ogc/coppa1.htm
http://www.ftc.gov/privacy/privacyinitiatives/COPPARule_2005SlidingScale.pdf

Principles:

Notice, Minimum Necessary and Limited Use, Consent, Security Safeguards

1.15. Cable Communications Policy Act (CCPA)
47 U.S.C. § 551, Pub. L. 98-549

Description:

The Cable Communications Policy Act protects the personal customer information held by cable service providers. Pursuant to the CCPA, cable service providers must obtain prior written or electronic consent from a subscriber before collecting any personal information. Consent is not required to obtain information "necessary to render cable services;" nor is it required for information used to detect unauthorized reception. Disclosure also generally requires prior consent, with the same two exceptions for business necessity and detection of cable piracy. Disclosure of personal information without consent is also permitted pursuant to a court order. The subscriber must be notified, and offered an opportunity to appear and contest the order. Disclosures may not generally include information about the subscriber's particular selections of video programming.

A cable service provider must destroy personal information when it is no longer needed for the purposes for which it was collected (and there are no pending requests for access). It must take appropriate steps to prevent unauthorized access of customers' personal information for as long as it is held.

Any person may bring a civil action against a cable provider for violations of this section and may seek actual and punitive damages.

CCPA specifically includes such "other services" as "radio and wire communications," which likely would include providers of cable broadband Internet service. The provisions of the CCPA probably cannot be stretched to apply to direct broadcast satellite (DBS) service even though they provide functionally similar services.

Implications:

Under the CCPA, Departments, and particularly colleges and universities who are or may be cable service providers, must provide a written notice of privacy practices to each subscriber (customer) at the time of entering into a service contract and at least once a year thereafter. The privacy notice must specify:

- The nature of the personally identifiable information that is or may be collected, and the uses to which it may be put.
- The "nature, frequency and purpose" of any disclosure that may be made of such information, including identification of the persons to whom those disclosures may be made.
- How long the information may be maintained by the cable service provider.
- Where and how the subscriber may have access to the information about him- or herself.
- The subscriber's right to bring legal action if the requirements of the law are not followed.

Note:

States are not preempted from enacting laws which provide greater privacy protections than the CCPA.

Sources:

http://www4.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000551----000-.html
http://www.consumerprivacyguide.org

Principles:

Security Safeguards, Consent, Notice, Individual Rights, Minimum Necessary and Limited Use

1.16. Video Privacy Protection Act
18 U.S.C. § 2710

Description:

The Video Privacy Protection Act of 1988 as originally passed created one of the strongest consumer privacy protection laws prohibiting disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual material." The Act has several provisions, including:

- A general ban on the disclosure of personally identifiable rental information unless the consumer consents specifically and in writing.
- Disclosure to police officers only with a valid warrant or court order.
- Disclosure of "genre preferences" along with names and addresses for marketing, but allowing customers to opt out.
- Exclusion of evidence acquired in violation of the Act.
- A requirement that video stores destroy rental records no longer than one year after an account is terminated.

Issues remain about the applicability of the Act to other rental records, including DVDs and video games, which are commonly rented by the same stores that rent video cassettes. The plain language of the Act would indicate that it applies broadly to all such records, but no cases have interpreted the language. Since the passage of the U.S. Patriot Act, which expands law enforcement powers to permit use of administrative subpoena or otherwise procure information such as library records and individual purchasing records "in the course of an ongoing investigation" (a lower standard than the traditional warrant), it is unclear whether this Act's ban is circumvented by the use of administrative subpoena.

A person may sue for violations of VPPA, including actual damages (statutorily not less than $2,500.00), punitive damages, and attorney's fees.

Implications:

- Departments that provide video cassette rental services should develop policies implementing the protections of the VPPA.
- Departments that are subpoenaed or otherwise contacted by federal enforcement authorities requesting the disclosure of VPPA, protected material should contact the Attorney General and the State Privacy Officer.

Source:

http://www.law.cornell.edu/uscode/18/usc_sec_18_00002710----000-.html

Principles:

Security Safeguards, Minimum Necessary and Limited Use

1.17. United States Patriot Act
50 U.S.C. § 1861; 18 U.S.C. § 2702; Pub. L. 107-56

Description:
The Patriot Act, with amendments, was enacted to deter and punish terrorist acts in the United States and around the world. There are a number of provisions in the Act that relate to disclosure of information to the federal government in support of a variety of investigations.

50 U.S.C. § 1861 governs access to certain business records for foreign intelligence purposes and international terrorism investigations. According to the Act, the Director of the FBI or a designee may make an "application for an order requiring the production of tangible things for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." For each disclosure, "minimization procedures" are to be established, limiting the dissemination only to those individuals to whom disclosure is absolutely necessary. Tangible things can include library circulation records, library patron records, books sales records, customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person.

18 U.S.C. § 2702 governs voluntary disclosure of customer communications or records. Generally, the section states that an "entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." However, enactment of the Patriot Act created an exception to allow disclosure "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."

Note:

The Patriot Act was renewed by Congress for four (4) years – setting to expire on June 1, 2015.

Implications:
- Departments are subject to the disclosure requirements or parameters identified in the Patriot Act. There is limited case law interpreting the Patriot Act and how it relates to state or federal privacy laws.
- Departments that are subpoenaed or otherwise contacted by federal enforcement authorities requesting the disclosure of otherwise protected material should contact their designated attorney and Privacy Officer.

Sources:
http://ithandbook.ffiec.gov/resources/outsourcing-technology-services.aspx
http://www.law.cornell.edu/uscode/html/uscode50/usc_sec_50_00001861----000-.html
http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002702----000-.html

Principles:
Minimum Necessary and Limited Use

1.18. Computer Fraud and Abuse Act of 1986 (CFAA)
18 U.S.C. § 1030

Description:

This law was passed in 1986 and was intended to reduce "hacking" of computer systems. It applies to any "protected computer," which is any computer used in interstate or foreign commerce or communication by the federal government, a federally regulated financial institution or any private computer system network spanning more than one state. CFAA provides for criminal and civil liability for accessing a protected computer without authorization and obtaining anything of value. If the only thing of value is the use of the computer, the value of such use must be greater than $5,000 during any one-year period.

The Act prohibits the following:

- To knowingly access a computer without authorization, or in excess of authorization, in order to obtain classified United States defense or foreign relations information with the intent to harm the United States or benefit a foreign nation.
- To obtain information, via unauthorized access, from the financial records of a financial institution or from any protected computer if the conduct involves interstate or foreign communication.
- To access a computer to use, destroy, modify, or disclose information found in a "federal interest" computer system, as well as to prevent authorized use of any computer used for government business if the usage interferes with government activities.
- To knowingly, and with the intent to defraud, participate in the trafficking of passwords or similar information through which computers can be accessed without authorization.

This law was amended in 1994, 1996 and in 2001 by the U.S. Patriot Act. The U.S. Patriot Act increased the scope and penalties of the CFAA by:

- Raising the maximum penalty for violations to 10 years (from 5) for a first offense and 20 years (from 10) for a second offense.
- Ensuring that violators only need to intend to cause damage generally, not intend to cause damage or other specified harm over the $5,000 statutory damage threshold.
- Allowing aggregation of damages to different computers over a year to reach the $5,000 threshold.
- Enhancing punishment for violations involving any (not just $5,000) damage to a government computer involved in criminal justice or the military.
- Including damage to foreign computers involved in U.S. interstate commerce.
- Including state law offenses as priors for sentencing.
- Expanding the definition of loss to expressly include time spent investigating and responding for damage assessment and for restoration.

The jurisdiction to investigate cases under this law is assigned jointly to the FBI and the U.S. Secret Service (USSS). The FBI is assigned to investigate cases involving espionage, misuse of classified data, government related fraud, terrorism, bank fraud, wire fraud and organized crime. The USSS has been given oversight responsibility for investigations of federal interest crimes relating to a variety of offenses, including financial institution fraud and electronic crimes involving network intrusion, where funds and data are stolen or manipulated.

Note:

This is parallel to the West Virginia Computer Crime and Abuse Act governing misconduct in West Virginia. West Virginia's statute prohibits the modification, destruction, access to, duplication of, or possession of data, documentation, or computer programs without the consent of the owner. The disclosure of restricted access codes or other restricted information to unauthorized persons is prohibited, and generally the degree of punishment or the magnitude of the fine is based on the degree of damage or cost. There is no breach reporting requirement.

Implications:

- Departments must assess current computer privacy policies.
- Departments must implement and develop policies in light of West Virginia's computer crime law to prevent computer fraud and abuse.

Sources:

http://www.law.cornell.edu/uscode/text/18/1030
http://www.justice.gov/criminal/cybercrime/reporting.html#C4

Principles:

Security Safeguards, Minimum Necessary and Limited Use, Consent

1.19. National Crime Prevention and Privacy Compact (NCPPC)
42 U.S.C. § 140, Subchapter II, §§ 14611—14616

Description:

The NCPPC creates an electronic information sharing system whereby the FBI and participating states can exchange criminal records for non-criminal justice purposes authorized by federal or state law, and provides reciprocity among the states to share records in a uniform fashion without charging each other for information. The Compact became effective in 1999. States participate following ratification of the Compact. West Virginia ratified the compact in 2006.

Implications:

- The West Virginia authorized criminal record repository must make all unsealed criminal history records available in response to authorized, noncriminal justice requests.
- Records received from other states must be screened to delete any information not otherwise permitted to be shared under West Virginia law.
- Records produced to other states are governed by the NCPPC and not West Virginia state law.

Source:

http://www.law.cornell.edu/uscode/html/uscode42/usc_sup_01_42_10_140_20_II.html

http://bjs.ojp.usdoj.gov/content/pub/pdf/ncppcrm.pdf

Principles:

Minimum Necessary and Limited Use

1.20. Genetic Information Nondiscrimination Act of 2008 (GINA)
Pub. L. 110-233 (signed into law May 21, 2008)
Internal Revenue Service, Department of Labor and Department of Health and Human Services joint regulations under Title I of GINA – 26 CFR Part 54, 29 CFR Part 2590 and 45 CFR Parts 144, 146 and 148; and Equal Employment Opportunity Commission regulations under Title II of GINA – 29 CFR Part 1635

Description:

This law is designed to prohibit the improper use of genetic information in health insurance and employment. It prohibits group health plans and health insurers from denying coverage to a healthy individual or charging that person higher premiums based solely on a genetic predisposition to developing a disease in the future. The legislation also bars employers from using individuals' genetic information when making hiring, firing, job placement, or promotion decisions. Employers with fifteen (15) or more employees and entities affecting commerce must display a GINA informational poster on their premises, describing that employment discrimination based on genetic information is against the law.

Title II of GINA prohibits covered employers from discriminating against employees based on genetic information. The Equal Employment Opportunity Commission (EEOC) issued regulations implementing Title II of the Act on November 9, 2010. These regulations are comprehensive. They describe or clarify:

1. Practices prohibited by GINA;
2. What constitutes "genetic information";
3. Examples of tests that would not be considered genetic tests;
4. Six narrowly-defined situations in which an employer may acquire genetic information;
5. Suggested warning language for employers to use when they request health-related information in the six narrowly-defined situations;
6. That there are no situations in which an employer may use genetic information to make employment decisions;
7. When acquisition of genetic information will be considered to be inadvertent;
8. What an employer must do to comply with GINA when lawfully requesting health-related information from an employee;
9. When an employer may ask for family medical history or other genetic information as part of a medical examination related to employment (*i.e*., a post-offer or fitness-for-duty examination);
10. What an employer must do when it offers employees or his or her family members health or genetic services, including wellness programs, on a voluntary basis;
11. Why GINA includes an exception that allows an employer to acquire family medical history as part of the Family Medical Leave Act certification;
12. Types of situations when an employer may lawfully acquire genetic information from sources that are commercially and publicly available;
13. Circumstances in which an employer may acquire genetic information through genetic monitoring of its workforce;

14. Employer acquisition of genetic information for law enforcement purposes or for human remains identification;

15. GINA's rules on confidentiality;

16. The prohibition of disparate impact claims under Title II of GINA;

17. The prohibition on harassment based on genetic information;

18. Application of Title II of GINA to employment decisions concerning health care benefits, including a "firewall" provision intended to eliminate "double liability" by preventing claims asserted under Title II from also being asserted under Title I of GINA;

19. That GINA does not preempt any state or local law that provides equal or greater protections from employment discrimination on the basis of genetic information or that provide greater privacy protections;

20. Remedies available against an employer for violation of GINA Title II; and

21. What happens when an employee files a charge under GINA with the EEOC against a private sector employer or a state or local government employer.

GINA expands Title VII of the Civil Rights Act of 1964 which already bans discrimination by race and gender to prohibit employers from discriminating against employees on the basis of "genetic information" in hiring, firing, and other activities. "Genetic information," not only includes tests that determine variations in a person's DNA, but also information regarding family history of a particular disease. GINA also prohibits employers from collecting genetic information from their employees, except for rare circumstances such as testing for adverse effects to hazardous workplace exposures, and requires strict confidentiality of genetic information obtained by employers. GINA grants employees and individuals remedies similar to those provided under Title VII and other nondiscrimination laws, i.e., compensatory and punitive damages. It also provides that no person shall retaliate against an individual for opposing an act or practice made unlawful by GINA. Currently, GINA does not prohibit discrimination once someone already has a disease.

The GINA is far-reaching in that it amends or touches upon many laws including the Employee Retirement Income Security Act of 1974 (ERISA), the Public Health Service Act, the Internal Revenue Code of 1986, Title XVIII (Medicare) of the Social Security Act, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). For example, it amends ERISA and the Public Health Service Act to prohibit health insurers from discriminating against individuals on the basis of genetic information. It also prohibits insurers from requiring genetic testing, tying premiums to genetic information, or considering family history of genetic disorders in making underwriting and premium determinations. The GINA also requires that all genetic information be treated as protected health information under HIPAA, thus making this information subject to HIPAA's Privacy Rule. The Office of Civil Rights has even extended GINA's prohibition on the use and disclosure of genetic information for underwriting to all entities covered by HIPAA.

Implications:

- Departments shall develop procedures in compliance with GINA.
- Departments possessing genetic information about its employees must keep the information confidential and stored in separate files.
- Departments must develop protocols to maintain the confidentiality of genetic information unless the disclosure is to one of the following: (1) to the employee upon request; (2) to a health researcher; (3) as directed by a court order; (4) to a government official investigating compliance with GINA; or (5) in connection with federal and state family and medical leave act provisions.

Source:

:

http://www.genome.gov/10002077
http://www.gpo.gov/fdsys/pkg/PLAW-110publ233/pdf/PLAW-110publ233.pdf

Principles:

Accountability, Minimum Necessary and Limited Use, Consent, Individual Rights, Security Safeguards

1.21. Real ID Act of 2005
P.L. 109-13 (signed into law May 11, 2005)

Description:

The REAL ID Act is a nationwide effort intended to prevent terrorism, reduce fraud, and improve the reliability and accuracy of identification documents that state governments issue. This law imposes certain security, authentication and issuance procedures standards for states' driver's licenses and state ID cards, in order for them to be accepted by the federal government for "official purposes", as defined by the Secretary of Homeland Security. Currently, the Secretary of Homeland Security has defined "official purposes" as presenting state driver's licenses and identification cards for boarding commercially operated airline flights, entering federal buildings and nuclear power plants. The Act is a rider to an act titled Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005.

The final rule requires the states to have a comprehensive security plan for offices that have DMV records and information systems. The plan must safeguard personally identifiable information collected, stored, or disseminated for purposes of complying with the REAL ID Act, including procedures to prevent unauthorized access, use, or dissemination of applicant information and images of source documents. The regulations include standards and procedures for document retention and destruction. Also, the regulations include standards for the information and security features that must be incorporated into the ID card.

At present, all state issued licenses and identification cards have phased implementation dates commencing
December 1, 2014.

Note:

See also, Section 1.10 Driver's Privacy Protection Act

Implications:

- The Departments shall work with leadership to develop a driver's license and identification card in compliance with the Real ID Act's requirements.
- The Real ID Act anticipates the exchange of driver identity data, document imaging, digital photographs and driver record information among all states accompanied by proper restrictions on any outside access or improper usage.

Source:

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ013.109.pdf
http://edocket.access.gpo.gov/2008/08-140.htm

Principles:

Accountability, Notice, Minimum Necessary and Limited Use, Security Safeguards

1.22. Electronic Communications Privacy Act of 1986
18 U.S.C. § 2701, et seq.; 47 U.S.C. § 605; 47 U.S.C. § 605

Description:

This law was enacted to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer. The Act prohibits persons from tampering with computers or accessing certain computerized records without authorization. The Act also prohibits providers of electronic communications services from obtaining, altering or preventing authorized access to stored electronic communications (Title II is known as the Stored Communications Act). This Act usually requires that the customer be notified and give an opportunity to contest in court a government entity's request for access to electronic mail or other stored communications in control of a provider of electronic communications services or remote computing services.

While the Act is, in part, a criminal anti-hacking statute, it also provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." The Act directly prohibits the interception of e-mail transmissions. Interception is prohibited by (1) unauthorized individuals or (2) individuals working for a government entity, acting without a proper warrant. While there is no specific prohibition in the Act for an employer to monitor the e-mail of employees, it does not specifically exempt employers.

The Act has several exceptions to the application of the prohibition of interception of electronic communications. The three most relevant to the workplace are (1) where one party consents, (2) where the provider of the communication service can monitor communications, and (3) where the monitoring is done in the ordinary course of business.

Violators of the Act are subject to criminal penalties, which includes both fines and imprisonment. It also creates a civil cause of action for any "person aggrieved by any violation of this chapter" where the conduct constituting the violation "is engaged in with a knowing or intentional state of mind."

Implications:

- Departments will establish clear, concise policies limiting employees' privacy in their electronic communications while using workplace computer systems.
- Departments will notify employees of their limited expectation of privacy in their personal communications on the workplace service provider, and that the Department as the provider of the equipment and services, retains the right to monitor the equipment's usage.
- Departments should notify employees that anyone in violation of the Computer and Internet Use policies will be disciplined.
- Departments should have employees sign a written acknowledgement that they have received, read and accepted the computer usage policies.

Source:
18 U.S.C. § 2701, et seq.; 47 U.S.C. § 605; 47 U.S.C. § 605
http://www.law.cornell.edu/uscode/text/18/part-I/chapter-121
http://www.law.cornell.edu/uscode/text/47/605

Principles:
Notice, Consent

2.0. Federal Case Law

National Aeronautics and Space Administration v. Nelson, 131 S.Ct. 746 (2011)

The United States Supreme Court considered a case in which Plaintiffs alleged that NASA's "National Agency Check with Inquiries" employee background check process violated a constitutional right to informational privacy for contract employees. The forms at issue asked whether an employee had "used, possessed, supplied, or manufactured illegal drugs" in the last year. If so, the employee was required to provide details, including information about "treatment or counseling received." *Id*. at 748. An employee was also required to sign a release authorizing the Government to obtain personal information from schools, employers, and others during its investigation. The Government sent the employee's references a questionnaire asking open-ended questions about whether the references had "any reason to question" the employee's "honesty or trustworthiness," or have "adverse information" concerning a variety of other matters. *Id.* at 748-749. All responses on the forms were subject to the protections of the federal Privacy Act.

The Supreme Court reversed the Ninth Circuit's reversal of the district court's denial of a preliminary injunction. The Court determined that while the government's challenged inquiries implicated a privacy interest of constitutional significance, that interest did not prevent the government from asking reasonable questions of the sort included on the forms at issue in an employment background investigation that was subject to the Privacy Act's safeguards against public disclosure. *Id.* at 757.

Specifically, the Court noted that the challenged questions were reasonable, employment-related inquiries that further the Government's interests in managing its internal operations. The "treatment or counseling" question was a follow-up question to a reasonable inquiry about illegal-drug use. The drug-treatment inquiry was also a reasonable, employment-related inquiry. Further, the form's open-ended questions were reasonably aimed at identifying capable and reliable employees. *Id.* at 761. The Court concluded: "the Government has an interest in conducting basic employment background checks. Reasonable investigations of applicants and employees aid the Government in ensuring the security of its facilities and in employing a competent, reliable workforce." *Id*. at 758.

The Court found significant that the answers to the Government's background check forms were subject to substantial protections against disclosure to the public. The Court noted that the Privacy Act allows the Government to maintain only those records "relevant and necessary to accomplish" a purpose authorized by law and requires written consent before the Government may disclose an individual's records. *Id.* at 762.

Implications:

The Supreme Court's decision confirms that Departments may request a broad range of background information from employees or applicants, as long as the inquiry is related

to the Department's interest in employing a competent workforce. However, Departments must take meaningful steps to comply with state and federal privacy laws and protect collected confidential information collected from disclosure.

FCC v. AT & T Inc., 131 S. Ct. 1177 (2011)

CompTel, a trade association representing some of AT&T's competitors, filed a FOIA request with the Federal Communications Commission (FCC) seeking all documents related to an FCC investigation into whether AT&T had overbilled the government for certain services. AT&T challenged the request, contending that the production would violate Exemption 7(c) of FOIA, which exempts document disclosures in law enforcement records which would constitute an invasion of "personal privacy."

The FCC rejected AT&T's argument that it was a "corporate citizen" with personal privacy rights and held that Exemption 7(C) applied only to individuals. The United States Court of Appeals for the Third Circuit held that the phrase "personal privacy" applied to corporations because other sections of FOIA had defined "person" to include a corporation. The Supreme Court reversed the lower court decision and held that corporations do not have a right of personal privacy for the purpose of Exemption 7.

Milner v. Department of Navy, 131 S. Ct. 1259 (2011)

The member of an organization dedicated to raising community awareness of dangers of the Navy's explosions activities brought an action under the Freedom of Information Act (FOIA) to obtain the release of Navy documents relating to the effects of explosions at particular locations. The parties moved for summary judgment on the topic of whether FOIA Exemption 2, which protects from disclosure material "related solely to the internal personnel rules and practices of an agency," applied to preclude the production. The Supreme Court held that Exemption 2 shields only those records relating to "personnel rules and practices" and that the key statutory word "personnel" refers to human resources matters. Because Exemption 2 encompasses only records relating to employee relations and human resources issues, the requested explosives data did not qualify for withholding under that FOIA exemption.

Implications:

These decisions should be considered when interpreting any similar provisions within West Virginia's Freedom of Information Act.

City of Ontario v. Quon, 130 S.Ct. 2619 (2010)

Ruling:

The U.S. Supreme Court unanimously upheld the legality of the Ontario, California Police Department's audit of a police sergeant's text messages in his department-issued pager. Declining to issue a broad holding on employee privacy rights in electronic communications, the Court decided the case on the narrow point that, even assuming that the employee had a reasonable expectation of privacy in his text messages, the search was reasonable because it was motivated by a legitimate, work-related purpose and was not excessive in scope. Nonetheless, the opinion emphasized the importance of well-crafted employer privacy policies, noting that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."

The *Quon* decision contained additional comments by the Court:

- The Court, in light of the department's policy in this case, highlighted the distinction between e-mails that are transmitted through a company's own server and text messages that are transmitted through a wireless provider's network, but ultimately concluded that the policy covered both;
- The Court noted that the department's audit of Quon's text messages on his employer-provided pager was "not nearly as intrusive as a search of his personal e-mail account or page, or a wiretap on his home phone line";
- The Court noted with approval the City's removal of the employee's off-duty messages from the audit and confining the audit to two months;
- The Court made clear that it has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."

Implications:

- Departments should either clarify and update or implement written policies covering all forms of electronic communications and require written acknowledgements of receipt by employees.

- Department privacy policies should state that employees do not have an expectation of privacy in electronic communications sent or received on Department-provided devices and that the Department may monitor and review electronic communications sent on such devices, not just those sent through the Department's server.

- Privacy policies should state that they can only be amended in writing by certain specified individuals with designated authority and should provide that violations of the privacy policies may lead to discipline up to and including termination.

- Departments should consider whether their privacy policies pertaining to workplace monitoring and surveillance clearly state when (defining purpose and scope) Departments may conduct legitimate and reasonable searches of Department-provided service and equipment.

- Departments should provide training regarding the electronic communications policy to all employees.

- Departments should consider developing investigative protocols for vetting, conducting and limiting searches, documenting the purpose for such searches, and establishing minimization procedures in order to enhance the likelihood that such searches will be deemed compliant in light of *Quon* and in line with general privacy notions.

- Departments should confirm that the agreement between them and any electronic communications provider identifies the employer as the subscriber for purposes of the Electronic Communications Privacy Act.

West Virginia

3.1. Executive Order No. 6-06 (August 16, 2006)

Description:

Executive Order No. 6-06 rescinds and supersedes Executive Order No. 7-03. Order 6-06 designates the Health Care Authority Chairperson as the person responsible for protecting the privacy of confidential and personally identifiable information, collected and maintained by Executive Branch Departments. The Chief Technology Officer (CTO) is responsible for information security for the Executive Branch Departments.

The HCA Chair is empowered to develop a privacy program, to create and maintain a privacy team, to issue privacy policies, to develop and implement data classification schemes and to develop measures to remediate, as appropriate, following privacy audits.

The CTO is to create an information security team to oversee the development and supervision of security policies, data classification schemes and measures to remediate, as appropriate, following security audits.

Implications:

- An Executive Branch Privacy Management Team, chaired by HCA, is created with representation from each Department. Each Executive Branch Department must designate a Privacy Officer who shall actively participate on the Team.
- The Team shall raise privacy awareness, perform privacy assessments, determine privacy requirements, and implement appropriate policies and procedures.
- The Team shall look for opportunities to improve the protection of private information, including:
    - Restricting disclosure of personal information;
    - Increasing individual access to personal information;
    - Granting individuals the right to seek amendment of personal information;
    - Establishing a State government policy for the collection, maintenance and dissemination of personal information; and,
    - Compliance with privacy laws, including HIPAA and other federal and State mandates.

Source:

http://www.privacy.wv.gov/privacy-program/Documents/Executive%20Order%206-06.pdf

Principles:

Accountability, Minimum Necessary and Limited Use, Individual Rights, Security Safeguards

3.2. Freedom of Information Act
W. Va. Code § 29B-1-1 *et seq*.

Description:

This law mandates that "[e]very person has a right to inspect and copy any public record of a public body in this State, except as otherwise" exempted.

The Legislature exempts "[i]nformation of a personal nature such as that kept in a personal, medical or similar file, if the public disclosure thereof would constitute an unreasonable invasion of privacy, unless the public interest by clear and convincing evidence requires disclosure in the particular instance." An individual can always inspect and copy his or her own records.

Additionally, information may be specifically exempted from disclosure by another statute; *see e.g.,* discussion regarding the Records Management and Preservation of Essential Records Act which protects certain PII. Also exempted from FOIA disclosure are computing, telecommunications and network security records, passwords, security codes or programs used to respond to or plan against acts of terrorism which may be the subject of a terrorist act. In 2009, House Bill 2418 exempted information relating to the design of corrections and jail facilities, and policies and procedures relating to the safe and secure management of inmates. There are a total of seventeen exemptions which may be asserted by an agency.

In 2011, House Bill 2475 amended the 2009 amendment to also exempt the design of detention facilities and the Division of Juvenile Services beginning May 17, 2011.

There is a private right of action; there are criminal penalties and attorney fees and costs may be awarded for violations of the Act.

Implications:

- Departments shall ensure that their responses to FOIA requests do not include PII or medical information that is exempt from FOIA.
- Departments shall ensure that their responses to FOIA do not include any other exempted or confidential information, without the approval of their Department head. *See* West Virginia Privacy Case Law.

Source:

http://www.justice.gov/oip/foia_guide09.htm
http://www.legis.state.wv.us/WVCODE/Code.cfm?chap=29b&art=1

Principles:

Individual Rights and Individual Participation, Security Safeguards, Minimum Necessary and Limited Use

3.3. Records Management and Preservation of Essential Records Act
W. Va. Code §§§ 5A-8-5, 21, 22

Description:
West Virginia law requires State government to safeguard certain personal identifying information with respect to State employees and citizens, and to disclose to non-governmental entities only as authorized by law. With regard to State officers, employees, retirees or the legal dependents thereof, the following individual identifiers are confidential and exempt from disclosure: home address, SSN, credit or debit card numbers, driver's license number and marital status or maiden name. With regard to individuals generally, the following individual identifiers are confidential and exempt from disclosure: SSN and credit or debit card number.

The State government must also establish and apply efficient methods to the creation, utilization, maintenance, retention, preservation and disposal of state records.

Implications:
- Departments must establish procedures to ensure that these identifiers are safeguarded and kept confidential.
- Departments must establish procedures to ensure that these personal identifiers are protected from disclosure to non-governmental entities, unless the disclosure is authorized by law. Procedures regarding FOIA should be reviewed to ensure conformance with these laws.
- Departments must establish policies and procedures governing record retention and disposal of varying types of state records as permitted by applicable law.

Source:

http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=8&section=5#08
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=8&section=21#08
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=8&section=22#08

Principles:
Minimum Necessary and Limited Use, Security Safeguards, Accountability

3.4. Information Services and Communications Division
W. Va. Code §§ 5A-7- 1, 11

Description:
The Division of Information Services and Communications of the Department of Administration establishes, develops and improves data processing and telecommunication functions in the various Departments and promulgates standards in the utilization of data processing and telecommunication equipment.

Article 7 creates a specific privacy and security obligation: Under no circumstances shall the head of any department or agency deliver to the Division [of Information Services and Communications] any records required by law to be kept confidential, but such head may extract information from such records for data processing by the division, provided the integrity of such confidential records is fully protected.

Implications:
- Departments must develop protocols for removing confidential, personal information or identifiable health information prior to delivering requested data to the division.

Source:
W. Va. Code §§ 5A-7-1

http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=7&section=11#07

Principles:
Minimum Necessary and Limited Use, Security Safeguards

3. 5. The Uniform Electronic Transactions Act
W. Va. Code §39A-1-1 *et seq*.

Description:

This law applies to transactions between parties where both have agreed to use electronic records and signatures. “Transaction” means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial or governmental affairs. The Act creates a duty to give notice in certain circumstances. The Act does not apply to wills and other testamentary writings, court orders or most UCC transactions. It also does not apply to the cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or recall of a product, or material failure of a product, that risks endangering health or safety; or any document required to accompany any transportation or handling of hazardous materials, pesticides or other dangerous materials.

If a statute, regulation or other rule of law requires that information relating to a transaction be provided or made available to a consumer in writing, the use of an electronic record to provide or make available such information satisfies the requirement that such information be in writing if: The consumer has affirmatively consented to such use and the consumer, prior to consenting, has been provided clear notice which states:

1. The consumer’s right or option to have the record provided or made available on paper or in non-electronic form.
2. The right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any consequences, which may include termination of the parties' relationship, or fees in the event of such withdrawal.
3. Informs the consumer of whether consent applies to a particular transaction or categories of records.
4. Describes how the consumer can withdraw consent.
5. How the consumer may obtain a paper copy and fees, if any, for the paper copy.

Once consent has been given, the consumer must be notified if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent.

Implications:

- Departments engaging in transactions with the public must develop appropriate notice and consent documents upon moving to electronic transactions.
- Departments must develop a method to store the consent or withdrawal of consent documents.

Source:

http://www.legis.state.wv.us/WVCODE/Code.cfm?chap=39a&art=1

Principles:

Notice, Consent, Individual Rights

3.6. State Health Privacy Laws

Description:

The West Virginia Code is a patchwork quilt of provisions governing the confidentiality of health related information. The HIPAA preemption analysis on the website references and summarizes the health-related confidentiality laws.

Implications:

- Departments collecting, using or disclosing health related information must ensure that they have procedures in place to carry out the mandated confidentiality and other privacy aspects.
- Departments collecting, using or disclosing health related information in conjunction with third-parties, must have Business Associate Agreements.

Source:

http://www.privacy.wv.gov/resources/HIPAA/Pages/WVPreemptionAnalysis.aspx

Principles:

Consent, Individual Rights, Minimum Necessary and Limited Use, Security Safeguards, Accountability

3. 7. West Virginia Health Information Network
W.Va. Code §16-29G-1 *et seq***.**

Description:

The West Virginia Health Information Network, under the oversight of the West Virginia Health Care Authority, is created to promote the design, implementation, operation and maintenance of a fully interoperable statewide network to facilitate public and private use of health care information in the State. As part of its duties, the Health Care Authority "shall ensure" that patient-specific protected health information be disclosed only in accordance with the patient's authorization or best interest to those having a need to know, in compliance with State confidentiality laws and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The health information, data and records of the network shall be exempt from disclosure under FOIA.

Implications:

- Departments and private participants in the network must work with the Authority to protect the privacy of patient-specific health information.

Source:

W.Va. Code §16-29G-1

Principles:

Accountability, Consent, Individual Rights, Minimum Necessary and Limited Use, Security Safeguards

3.8. Maxwell Governmental Access to Financial Records Act
W. Va. Code § 31A-2A-1 *et seq*.

Description:

This law sets forth the conditions under which a financial institution (bank, savings and loan association, a trust company or a credit union) may disclose a customer's financial records to a State entity and the conditions under which a State entity may have access to or obtain those records. Examples of appropriate access include customer authorization, legal process, law enforcement resulting from a criminal investigation, and as required or permitted by any other State or federal law. A State entity that receives information in accordance with the procedure set forth in the Act may not disclose financial records to any other State entity or any other person unless the receiving State entity or other person is authorized by law or by the customer to receive the records. This law, however, does not prevent a receiving State entity from disclosing properly obtained financial records "to facilitate a lawful proceeding, investigation, examination or inspection by a state entity." Financial institutions are required to obtain written certification from the receiving State entity that it has complied with the applicable provisions of this law.

There are 18 exceptions to this law; examples include banking and insurance regulatory activities and various disclosures to DHHR regarding eligibility for public assistance and the federal parent locator service.

There are criminal and civil penalties for violations of this law. There is also a private right of action.

Implications:

- Departments that have financial institution operations shall ensure that they have policies and procedures governing the disclosure of customer financial records to any State entities.
- Departments that obtain customer's financial records shall ensure that they have policies and procedures regarding disclosure of the records.

Source:

W. Va. Code § 31A-2A-1

Principles:

Consent, Minimum Necessary and Limited Use

3.9. Confidentiality and Disclosure of Tax Returns and Return Information

W. Va. Code §§ 11-10-5d, 11-10-5s, 11-10-5u, 11-10-5v, 11-10-5w, 11-10-5y, 11-13J-10, 11-13Q-20, 11-13R-11, 11-13S-10, 11-13U-8, 11-13AA-9, 11-13BB-11.

W. Va. C.S.R. §§ 110-50A-1, 110-50B-1, 110-50D-1, 110-50D-1, 110-50E-1, 110-50F-1 and 110-50G-1

Description:

Generally, tax returns, associated reports and declarations, and the information they contain are confidential and may not be disclosed to anyone, with certain enumerated exceptions. This law governs the Tax Department's disclosure of return information, as well as government, in general. Importantly, except for very specific situations, such as under a court order, the release of confidential information is at the discretion of the Tax Commissioner. Departments receiving return information will be required to enter into an exchange of information agreement with the Tax Department and safeguard the information as confidential. Tax return information is not subject to FOIA.

Disclosure may occur:

- When required by the Tax Commissioner in an official investigation.
- Where the Tax Commissioner is a party in a proceeding to determine the amount of tax due.
- When the taxpayer authorizes disclosure to an individual,
- For use in criminal investigations.
- To a person having a material interest, as defined by the Tax Commissioner in regulations.
- For statistical use.
- Regarding disclosure of the amount of an outstanding lien to such person who has a right in the property subject to the lien or intends to obtain a right.
- For reciprocal exchange in the administration of tax programs.
- In administrative decisions; however, identifying characteristics or facts about the taxpayer shall be omitted or modified so the name or identity of the taxpayer is not disclosed.
- When the Tax Commissioner determines that certain taxpayer information (such as those who have a current business registration certificate, those who are licensed employment agencies, etc.) should be released to enhance enforcement.
- To the Bureau for Child Support Enforcement.
- For purposes of jury selection.
- As required to be disclosed by W. Va. Code § 11-10-5s.
- Regarding names of persons making retail sales of tobacco products.
- To the State Treasurer for return, recovery and disposition of unclaimed and abandoned property.
- To county assessors, Department of Environmental Protection and the Public Service Commission regarding certain oil and gas production information.
- To the Consolidated Pension Retirement Board.

- Regarding certain information pertaining to neighborhood investment tax credit program.
- Regarding certain information about economic opportunity tax credit.
- Regarding certain information about strategic research and development tax credit.
- Regarding certain information about manufacturing investment tax credit program.
- Regarding certain information about high-growth business investment tax credit program.
- Regarding certain information about commercial patent incentive tax credit program.
- Regarding certain information about mine safety technology tax credit program.
- To Alcohol Beverage Control Administration.
- To Department of Labor, Department of Commerce, Commissioner of Insurance, Commissioner of Motor Vehicles, Commissioner of Employment Programs, Office of Governor, Department of Transportation and Department of Environmental Protection.
- To West Virginia Lottery.
- To State Fire Marshal.

There are criminal penalties for violation of this law.

Implications:

- The Tax Department must ensure that it has policies in place such that tax returns and related information are only disclosed in accordance with this law.
- Departments must assess whether they receive tax return information, and if they do, they must ensure that they have policies requiring that it be held confidentially and only disclosed in accordance with this law and the terms of the exchange of information agreement signed with the Tax Department.

Source:
W. Va. Code § 11-10-5d; ; W. Va. Code § 11-10-5s; W. Va. Code § 11-10-5u; W. Va. Code § 11-10-5v; W. Va. Code § 11-10-5y; W. Va. Code § 11-13J-10; W. Va. Code § 11-13Q-20; W. Va. Code § 11-13R-11; W. Va. Code § 11-13S-10; W. Va. Code § 11-13U-8; W. Va. Code § 11-13AA-9; W. Va. Code § 11-13BB-11.
W. Va. CSR §§ 110-50A-1; 110-50B-1; 110-50D-1; 110-50E-1; 110-50F-1; 110-50G-1.

Principles:
Consent, Minimum Necessary and Limited Use, Security Safeguards

3.10. Uniform Motor Vehicle Records Disclosure Act
W. Va. Code §§ 17A-2A-1 through 14

Description:
This law implements the federal Driver's Privacy Protection Act of 1994 to protect individual privacy by limiting the use and disclosure of personal information in connection with motor vehicle records, except as authorized by the individual or by law.

Implications:
- DMV must have procedures to ensure that personal information obtained in connection with the motor vehicle record is only used and disclosed as authorized by law or with the consent of the individual.
- Departments must assess whether they obtain personal information from DMV.
- Departments obtaining personal information from DMV must ensure that they have procedures detailing use and disclosure of the personal information, as well as record keeping requirements. Note: State law requires an individual's express consent for redisclosure.

Source:
W. Va. Code §17A-2A-1 through 14

Principles:
Consent, Minimum Necessary and Limited Use, Security Safeguards

3.12. Consumer Credit and Protection Act, General Consumer Protection
W. Va. Code § 46A-6-101 *et seq.*

Description:

This law prohibits "[u]nfair methods of competition and unfair or deceptive trade practices" and is similar to Section 5 of the Federal Trade Commission Act which gives the FTC the power to enforce promises made in privacy notices, as well as challenge unfair information practices which result in substantial injury to consumers. http://www.ftc.gov/privacy/privacyinitiatives/promises.html

There is a private right of action.

Implications:

- Departments must accurately represent privacy policies in privacy notices.
- Departments must comply with promises made in privacy notices.
- Departments cannot put consumers at risk without an offsetting benefit. For example, if a company collects PII without reasonable security measures and does not tell the consumers, it would constitute an unfair trade practice.
- Departments cannot retroactively materially change a privacy notice with respect to information already collected without express, affirmative, opt-in authorization.

Source:

W. Va. Code § 46A-6-101

Principles:

Notice, Consent, Minimum Necessary and Limited Use

3.13. W.Va. Computer Crime and Abuse Act
W.Va. Code § 61-3C-1 *et seq*.

Description:

This law defines crimes for misuse and abuse of computers and computer data. The Legislature specifically recognizes the public's "privacy interest" in being protected from computer abuse. The Act specifically applies to the State and its subdivisions. It is a felony to knowingly and willfully access any computer to execute any scheme to defraud or obtain money by fraudulent pretenses. It is a misdemeanor to knowingly and willfully access any computer to obtain services without an authorization to do so. There are numerous other crimes delineated in the statute which are either felonies or misdemeanors depending on the monetary value of the crime. Willful disruption of computer services or willful denial of computer services to an authorized user is a misdemeanor. Willfully obtaining, without authorization, confidential information is a misdemeanor as is obtaining employment and salary information or other personal information. It is a felony for a person to interrupt or impair the provision of medical services or other services provided by any State agency. The Act provides for a private right of action which may include a claim for punitive damages.

The definition of "computer" was amended in 2012 to include file servers, mainframe systems, desktop personal computers, laptop personal computers, tablet personal computers, cellular telephones, game consoles and any other electronic data storage device or equipment. *See* SB 385 (effective May 31, 2012).

Additionally, this definition of computer was added to article 8A, chapter 61 of the Code (preparation, distribution or exhibition of obscene matter to minors). *Ibid*.

Implications:

- Departments need to develop policies and procedures to ensure to the extent possible that their employees are in strict conformance with the appropriate and authorized uses for the State's computers and software.
- The Department of Administration should check with BRIM that there is coverage for civil suits brought against the State or its employees under this Act.

Source:

W.Va. Code § 61-3C-1

Principles:

Minimum Necessary and Limited Use, Security Safeguards

3.14. Bureau for Child Support Enforcement, Confidentiality
W.Va. Code §§ 48-18-131,122

Description:
All child support records are confidential and protected from release except as otherwise provided by law. In addition, the Bureau for Child Support Enforcement maintains a Central State Case Registry for child support orders, which is subject to privacy and confidentiality safeguards, at both the state and federal level. Information may be shared among designated agencies to determine child support amounts or assist with enforcement of support orders.

It is a misdemeanor to violate the confidentiality provisions.

Implications:
- Departments must adopt policies to safeguard their employees' child support orders.

Source:
W.Va. Code § 48-18-131, W.Va. Code § 48-18-122

Principles:
Minimum Necessary and Limited Use, Security Safeguards

3.15. Sharing of Domestic Violence Information
W. Va. Code § 48-27-206 (effective June 9, 2010)

Description:

This law coupled with the repeal of § 48-27-803 permits West Virginia law enforcement agencies, defined as: the state police, county sheriffs and deputies and municipal police departments, as well as the Department of Health and Human Resources and any other state agency that receives reports of child abuse not reported elsewhere; and any federal agency whose purpose includes enforcement, maintenance and gathering of criminal and civil records relating to federal domestic violence law to report information to the West Virginia Criminal Identification Bureau, the West Virginia Domestic Violence Database and other entities as permitted or required by law.

Implications:

- Departments will update policies to permit the reporting of domestic violence information to the appropriate entities as permitted or required by law.

Source:

http://www.legis.state.wv.us/Bill_Text_HTML/2010_SESSIONS/RS/BILLS/hb4361%20enr.htm
http://www.jrsa.org/dvsa-drc/west_virginia/index.shtml

Principles

Minimum Necessary Limited Use, Notice, Accountability

3.16. The Emergency Medical Services Act
W. Va. Code §16-4C-1 *et seq*.
64 W. Va. C.S.R. § 27-10.2.c.

Description:

The law establishes the Office of Emergency Medical Services under the Bureau for Public Health. The related rule requires the Office of Emergency Medical Services to "ensure the security and confidentiality of protected information within the Trauma and Emergency Medical Information System according to State and federal guidelines." In addition, according to this rule, regulations may be imposed setting forth the requisite standards and requirements of certification/recertification of Emergency Medical Service personnel, as well as the requirements that ambulance operators must meet. Upon submission of an application for such a position, background checks may be required. This rule clearly protects the results of such background checks from being released.

Implications:

- Departments must work with the Agency to assure confidentiality within the framework of an emergency.
- Departments should continue to monitor the implementation of pertinent regulations and confirm they are in compliance as to what types of information must be maintained as confidential.

Source:

W. Va. Code §16-4C-1
http://apps.sos.wv.gov/adlaw/csr/readfile.aspx?DocId=8432&Format=PDF

Principles:

Minimum Necessary and Limited Use, Security Safeguards

3.17. W.Va. Insurance Commissioner Rule, “Privacy of Consumer Financial and Health Information”
114 W. Va. C.S.R. § 57; 114 W. Va. C.S.R. § 62
W. Va. Code § 33-6F-1

Description:
These privacy rules apply to all licensed insurers, producers and other persons licensed or registered pursuant to Chapter 33 of the West Virginia Code. While this rule does not apply to State entities such as BRIM or PEIA, it does apply to insurance licensees who have contracted with the State to provide services. “Nonpublic personal information” is defined to include nonpublic personal financial information and nonpublic personal health information. A licensee may not disclose personal financial information to nonaffiliated third parties unless otherwise permitted by the law or rule. A licensee who must comply with HIPAA is deemed to comply with the provisions governing privacy of health information; otherwise licensees must maintain the confidentiality of health information and obtain written authorization prior to disclosing personal health information, which authorization can be electronic.

In addition, in accordance with the Gramm-Leach-Bliley Act, the Insurance Commissioner has developed rules for safeguarding customer information. Each licensee must have a written information security program. Nonpublic personal information, whether in paper or electronic format, is covered by this rule.

Implications:
- These rules apply to licensed insurers utilized by agencies.

Source:
W. Va. Code § 33-6F-1
114 W. Va. CSR Series 57
114 W. Va. CSR Series 62

Principles:
Security Safeguards, Consent

3.18. West Virginia Code § 33-4A1 et seq. All-Payer Claims Database

Description:

West Virginia Code § 33-4A-1 et seq. took effect in June of 2011. This statute provides for the creation of an all-payer claims database which collects, retains, uses and discloses information concerning the claims and administrative expenses of health care payers. The statute requires the database to be developed by the Insurance Commissioner, the Secretary of Health and Human Resources and the chairperson of the Health Care Authority. It provides for the safekeeping and protection of personal identifiers and the confidentiality of information contained in the database. It also provides that certain information provided by insurance companies to the West Virginia Insurance Commissioner is considered to be confidential and is therefore exempted from disclosure under the Freedom of Information Act. It also provides that the confidential information is not subject to subpoena or discoverable in a private civil action. Further, it provides conditions relating to the Insurance Commissioner's authority to release, share and receive documents otherwise treated as confidential.

On July 1, 2012, 114A W. Va. C.S.R. § 1 titled "All-Payer Claims Database – Privacy and Security Requirements" becomes effective. The rule requires the transmission of data and retention of data to be secured in a manner that prevents unauthorized access and ensures confidentiality, integrity and availability of all data transmitted to the all-payer claims database to be incompliance with the HIPAA Security and Privacy Rules.

Source:

http://www.legis.state.wv.us/WVCODE/Code.cfm?chap=33&art=4A#04A
http://apps.sos.wv.gov/adlaw/csr/readfile.aspx?DocId=23604&Format=PDF

Principles:

Individual Rights, Security Safeguards

3. 19. Breach of Security of Consumer Information Act
W. Va. Code §§ 46A-2A-101-105

Description:

This law applies to all legal entities and to governments and governmental subdivisions and agencies. Notice or substitute notice is required in the event of a "breach of the security of a system," that causes one to reasonably believe will result in identity theft or fraud. Breach of the security of a system is defined as "unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information… [and that is] part of a database of personal information." Personal information means the name of an individual linked to unencrypted and unredacted social security number, driver's license or state identification card, or financial account numbers.

Notice, which can be provided by mail, telephone or electronically, includes: a description of the categories of information reasonably believed to have been accessed or acquired by the breach; a telephone number or website that can be accessed for the purpose of providing the individual with information about the types of information maintained on the individual or all individuals; whether the entity had information on the specific individual; and information about credit reporting agencies and placing fraud alerts or security freezes. Substitute notice is permitted when the entity can demonstrate cost of notice would exceed fifty thousand dollars or affected class exceeds one hundred thousand persons or entity lacks sufficient contact information. An entity can follow its own, established notification procedures as long as notice is consistent with the Act. Entities following notification procedures in accord with their primary or functional regulator are deemed to be in compliance. The Act does not apply to Departments subject to Title V of the Gramm-Leach Bliley Act.

The Attorney General has exclusive authority to enforce this Act, including seeking civil penalties, by bringing an action in State Court.

Implications:

- Departments with existing breach notification procedures should review them for consistency with the Act.
- Departments without breach notification procedures should develop procedures in accord with this Act and applicable West Virginia Executive Branch Privacy Policies.
- Departments should review and consider whether breach notification requirements under HIPAA as amended by HITECH may be applicable on a case by case basis. *See* Sections 1.4.2 and 1.5.
- If a breach occurs, Departments should refer to West Virginia Executive Branch Procedure governing unauthorized disclosures: *Response to Unauthorized Disclosures*.

Source:
W. Va. Code §§ 46A-2A-101--105; §46A-6-104; §§ 46A-6L-101--105

Principles:
Accountability, Notice, Security Safeguards

3.20. West Virginia Governmental Ethics Act
W. Va. Code § 6B-1-1 *et seq.*

Description:

All West Virginia public officials and employees are prohibited from knowingly and improperly disclosing any confidential information acquired in the course of performing official duties. Officials and employees are also prohibited from using such confidential information to further one's personal interests or the interests of another.

Individuals found guilty of violating this section of the Act are guilty of a misdemeanor and can be sentenced to not more than six months in jail or fined no more than one thousand dollars or both.

Implications:

- Supervisors should continuously educate employees about the importance of identifying information that is confidential under State or federal law, rule or policy, and the scope of the proper uses of confidential information.

Source:

W. Va. Code § § 6B-2-5, 6B-2-10

Principles:

Accountability, Minimum Necessary and Limited Use, Security Safeguards

3.21. West Virginia Ratification of the National Crime Prevention and Privacy Compact (NCPPC)
W. Va. Code § 15-2-24a

Description:
The NCPPC creates an electronic information sharing system whereby the FBI and participating states can exchange criminal records for non-criminal justice purposes authorized by federal or state law, and provides reciprocity among the states to share records in a uniform fashion without charging each other for information. The Compact became effective in 1999. States participate following ratification of the Compact. West Virginia ratified the Compact in 2006. The West Virginia State Police Superintendent is charged with oversight and implementation of the Compact on behalf of the State.

Implications:
- The West Virginia authorized criminal record repository must make all unsealed criminal history records available in response to authorized, non-criminal justice requests.
- Records received from other states must be screened to delete any information not otherwise permitted to be shared under West Virginia law.
- Records produced to other states are governed by the NCPPC and not WV law.

Source:
W. Va. Code § 15-2-24a

Principles:
Minimum Necessary and Limited Use

3.22. Chief Technology Officer Duties Relating To Security of Government Information

W. Va. Code §5A-6-4a

Description:

The Chief Technology Officer (CTO) and the Office of Technology oversee the statewide coordination of technology for State spending units (not including the Legislature, Judiciary or State constitutional officers or in most aspects, the Department of Education). As part of the CTO's duty to ensure the security of State government information, including protecting the data communications infrastructure from unauthorized uses, intrusions or other security threats, the CTO is charged with developing policy and procedure to safeguard information systems, data and communications infrastructures, as well as defining the scope and regularity of security audits and which bodies are authorized to conduct security audits. The audits may include on-site visits, as well as reviews of all written security procedures and practices.

Legislation enacted in 2012 clarifies that the CTO is responsible for the cleansing of information technology equipment prior to its retirement or transfer. W. Va. Code § 5A-6-4 (as amended by SB 563, effective June 8, 2012).

Implications:

- Departments need to be prepared to respond to and fully cooperate with authorized security auditors.
- The CTO may direct specific remediation to mitigate findings of insufficient administrative, technical and physical controls.

Source:

W. Va. Code §5A-6-4a

Principles:

Security Safeguards

3.23. Monitoring Inmates Telephone Calls and Mail
W. Va. Code §§ 25-1-17 and 25-1-18

Description:
This legislation authorizes the Commissioner of Corrections to monitor, intercept, open, record, and copy telephone calls and mail to inmates of state correctional institutions. Inmates must be notified in writing of these potential actions. The contents of these communications may be disclosed to law enforcement agencies pursuant to an order of a court or administrative tribunal when necessary to investigate, prosecute, or prevent a crime; to safeguard the orderly operation of the correctional institution; or to protect persons from harm or the threat of physical harm. Attorney-client communications are exempt from these requirements.

Implications:
- The Department of Corrections must have policies in place to comply with these statutes.
- The Department of Corrections must give clear guidance as to when a court order shall be sought before notifying law enforcement officials.
- The Department of Corrections must retain recordings and copies of these communications at least three years, and then destroy in accordance with its record retention policy.

Source:
W. Va. Code § 25-1-17
W. Va. Code § 25-1-18

Principles:
Accountability, Notice

3.24. Drug Testing for Public Improvements
W. Va. Code §§ 21-1D-2; 21-1D-7b; 21-1D-8

Description:
This legislation requires any contractor that is awarded a contract to construct a public improvement to maintain a drug-free workplace policy. Not less than once per year, or upon completion of the project, every such contractor shall provide a certified report to the public authority which let the contract to show what educational efforts were undertaken with employees; what federally certified laboratory conducted the testing; and the number of positive and negative drug tests conducted at the time of pre-employment, upon reasonable suspicion, post-accident, and at random. Failure to comply with this law is a misdemeanor.

Implications:
- Public authorities must develop compliance efforts to assess the contractor's implementation of the drug-free workplace policy.
- Contractual documents shall be amended to include the requirement for the maintenance of a drug-free workplace policy by the contractor as well as all subcontractors doing business, municipalities, and their political subdivisions.

Source:
W. Va. Code § 21-1D-2; § 21-1D-7b; § 21-1D-8

Principles:
Accountability, Notice, Security Safeguards

3.25. Verifying Legal Employment Status of Workers
W. Va. Code §§ 21-1B-1 and 21-1B-7

Description:

This law places the responsibility on employers to verify the legal employment status of all persons who come into their employ and to report their employment to the appropriate governmental agencies. "Employer" is defined as any individual, person, corporation, department, board, bureau, agency, commission, division, office, company firm, partnership, council or committee of the state government, public authority, or political subdivision of the state or other business entity which employs individuals. The Labor Commissioner is authorized to access information maintained by any other state agency for the limited purpose of confirming the validity of a worker's legal status or authorization of work. There is a penalty for employer's failure to maintain certain records. The Commissioner is authorized to issue notices to employers to produce records or documents to verify the legal status of an employee and to terminate undocumented employees

Implications:

- Departments must have policies and procedures in place to verify the legal status of employees and prospective applicants for employment.
- Departments should give Notice to prospective applicants that a verification of legal status for employment will be conducted and what information may be accessed or disclosed as a result of such verification.

Source:

W. Va. Code § 21-1B-1 and § 21-1B-7

Principles:

Accountability, Notice

3.26. Address Confidentiality Program
W. Va. Code §§ 48-28A-101 through 48-28A-110
W. Va. C.S.R. §§ 153-37-1 *et seq*.

Description:

This law established an Address Confidentiality Program in the Secretary of State's Office pursuant to which persons attempting to escape from actual or threatened domestic violence, sexual assault or stalking may establish a designated address in order to prevent their assailants or probable assailants from finding them. A person may apply to the Secretary of State to participate in this program. Upon approval of the application, the Secretary of State assigns the applicant a designated address, which state and local agencies and courts of this State are required to accept for the purpose of creating a new public record. The designated address is used by the Division of Motor Vehicles on the applicant's driver's license or identification card and the designated address or a post office box may be used by the applicant for voter's registration purposes. Procedures are provided under which the applicant's residential or mailing address is available to law enforcement officers and to the head of a state agency or designee under prescribed circumstances. Disclosure may also be made pursuant to a court order. The program participant's application and supporting materials are not public records. Willful unauthorized disclosure is a misdemeanor punishable upon conviction by a fine or imprisonment in a regional jail. Participation in this program is renewable every four years unless participation is cancelled.

Implications:

- The Secretary of State was required to propose legislative rules for promulgation.
- Courts and agencies of this State that receive the participant's residential or mailing address from the Secretary of State are required to keep that information confidential.

Source:

http://www.legis.state.wv.us/WVCODE/Code.cfm?chap=48&art=28A#28A
http://apps.sos.wv.gov/adlaw/csr/readfile.aspx?DocId=19953&Format=PDF

Principle:

Security safeguards

3.27 Security of Capital Complex, Other State Facilities and of Sensitive or Critical Information.
W. Va. Code § 15-2D-3

Description:
Effective June 8, 2012, any service provider whose employees are regularly employed on the grounds or in the buildings of the Capitol Complex or who have access to sensitive or critical information may be required by the Director of the Division of Protective Services, Department of Military Affairs and Public Safety, to submit to a fingerprint-based state and federal background inquiry through the state repository, and require a new employee who is employed to provide services on the grounds or in the building of the Capitol Complex to submit to an employment eligibility check through E-verify. W. Va. Code § 15-2D-3(e).

After the contract for these services has been approved, but before any such employees are permitted to be on the grounds or in the buildings of the Capitol Complex or have access to sensitive or critical information, the service provider must submit a list of all persons who will be physically present and working at the Capitol Complex for purposes of verifying compliance with W. Va. Code § 15-2D-3.

All current service providers must, within ninety days of the amendment and reenactment of section 15-2D-3 on March 10, 2012, ensure that all of its employees who are providing services on the grounds or in the buildings of the Capitol Complex or who have access to sensitive or critical information submit to a fingerprint-based state and federal background inquiry through the state repository.

Any contract entered into, amended or renewed by an agency or entity of state government with a service provider must now contain a provision reserving the right to prohibit specific employees thereof from accessing sensitive or critical information or to be present at the Capitol Complex based upon results addressed from a criminal background check.

For purposes of section 3, the term “service provider” means any person or company that provides employees to a state agency or entity of state government to work on the grounds or in the buildings that make up the Capitol Complex or who have access to sensitive or critical information.

In accordance with the provisions of Public Law 92-544 the criminal background check information is to be released to the Director of the Division of Protective Services.

Implications:
All agencies with offices at the Capital Complex should ensure that its outside service providers working at the Capital Complex, or who will work at the Capital Complex, or who will have access to sensitive or critical information comply with the new requirements of W. Va. Code § 15-2D-3.

Source:
SB 659, passed March 10, 2012 and effective June 8, 2012.
http://www.legis.state.wv.us/Bill_Status/bills_text.cfm?billdoc=SB659%20SUB1%20enr.htm&yr=2012&sesstype=RS&i=659

Principle:
Security safeguards

4.0. Agency Agreements with Privacy or Security Provisions

Description:

State Government contracts with vendors for products and services may require the vendor to receive or create PII or other confidential information including, but not limited to, a requirement to notify the State agency of a breach of security or privacy. Where a vendor receives or creates PII or other confidential information from or on behalf of the State, the vendor shall receive notice of the State's policy regarding the security and privacy of the information and agree to certain terms and conditions. Further, where the contracting Department is either a Covered Entity or Business Associate and PHI is or may be disclosed to the vendor, the Department shall ensure the vendor agrees to and executes the State Government Business Associate Addendum.

Implications:

- Departments shall ensure that the Purchasing Division's General Terms & Conditions are included within all contracts. The General Terms & Conditions are located at http://www.state.wv.us/admin/purchase/TCP.pdf. Use of the Purchasing Division's forms will facilitate compliance. Departments shall ensure that the West Virginia State Government HIPAA Business Associate Addendum, located at http://www.state.wv.us/admin/purchase/vrc/WvBaaAgApproved.pdf is also included in all contracts. Use of the Purchasing Division's forms will facilitate compliance.
- Departments which must be HIPAA compliant should assure that their business associates are in compliance with this Business Associate Addendum.
- Those acting as Business Associates will review and revise their policies, procedures, and practices in light of the HITECH Act amendments to HIPAA, all applicable regulations and any subsequently issued applicable regulations.
- Departments will monitor the law and attain compliance within the specified time periods as may be applicable.

Source:

http://www.state.wv.us/admin/purchase/vrc/WvBaaAgApproved.pdf
http://www.state.wv.us/admin/purchase/privacy/baa_notice.pdf
http://69.175.53.6/register/2010/jul/14/2010-16718.pdf

Principles:

Accountability, Security Safeguards, Notice, Individual Rights

4.1. Vendor Agreement Clauses

Description:

The HIPAA Business Associate Addendum approved by the Attorney General's Office, on August 2, 2010, is made a part of State agency contracts where the vendor is a "Business Associate" as that term is broadly defined in 45 CFR 160.103. In general, any vendor that will directly or indirectly have access to PHI is a business associate.

This Addendum, among other things:

1. Prohibits the Business Associate from using or disclosing PHI in a manner in violation of existing law and specifically in violation of laws relating to confidentiality of PHI, including but not limited to, the Privacy and Security Rules. HIPAA Business Associate Addendum Section 3 (obligations of associate), Subsection (d) (compliance with law).

2. Obligates the Business Associate to mitigate, to the extent practicable, any harmful effect that is known to the Associate of a use or disclosure of PHI by the Business Associate in violation of the requirements of the Business Associate Addendum, and to report its mitigation activity back to the applicable State agency. HIPAA Business Associate Addendum Section 3 (obligations of associate), Subsection e (mitigation)

3. Obligates the Business Associate to take all steps necessary to ensure the continuous security of all PHI and data systems containing PHI. HIPAA Business Associate Addendum Section 3 (obligations of associate), Subsection k (security).

4. Obligates the Business Associate to notify the applicable State agency and unless otherwise directed by the applicable agency, in writing, the Office of Technology immediately by telephone call plus e-mail, web form or fax upon the discovery of breach of security of PHI, where the use or disclosure is not provided for in the Business Addendum or was acquired by an unauthorized person, or within 24 hours by e-mail or fax of any suspected incident, unauthorized use or disclosure in violation of Business Addendum or potential loss of confidential data affecting the Addendum. HIPAA Business Associate Addendum Section 3 (obligations of associate), Subsection l (notification of breach).

5. Additionally the Business Associate is required to immediately investigate the Security incident, breach or unauthorized use or disclosure of PHI or confidential data and notify the applicable State agency contract manager in writing, within 72 hours, regarding (a) What data elements were involved and the extent of the data involved in the breach; (b) A description of the unauthorized person known or reasonably believed to have improperly used or disclosed PHI or confidential data; (c) A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or

utilized; (d) A description of the probable causes or the improper use or disclosure; and (e) Whether any federal or state laws requiring individual notifications of breaches are triggered. *Ibid*.

Because the Attorney General approves as to form purchasing contracts, the HIPAA Business Associate Addendum is most likely incorporated into all vendor contracts with a government agency, such as BMS, the Office of Insurance Commissioner, PEIA, or any other agency that has HIPAA information, when the vendor will directly or indirectly have access to that HIPAA information. See the first paragraph of the HIPAA Business Associate Addendum.

Additionally, the State Purchasing Division's Instructions to Vendors Submitting Bids requires vendors to agree to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws. *See* paragraph 45 (indemnification), Purchasing Division's General Terms and Conditions, Instructions to Vendors Submitting Bids, at http://www.state.wv.us/admin/purchase/TCP.pdf

5.0 West Virginia Case Law

The Associated Press v. Canterbury, 688 S.E.2d 317 (W. Va. 2009)

Ruling:

The West Virginia Supreme Court of Appeals held that a personal e-mail communication sent from a government e-mail account by a public official or public employee, which does not relate to the conduct of the public's business, is not a public record subject to disclosure under FOIA. The Court determined that e-mail is a "writing" and therefore a public record for purposes of FOIA analysis. In response to a public official's refusal to produce FOIA-requested records, a trial court may, in its discretion and on its own motion, order the production of records withheld by a public official. The trial court then reviews the records to determine whether any of the records are subject to disclosure under FOIA. This analysis is restricted to the content of the e-mail and is not driven by the context; that is, how and where the e-mail was created.

Implications:

The Court's holding establishes that public employees can expect some degree of privacy from public scrutiny when sending e-mail messages of a personal nature from work accounts. The analysis hinges on the Court's interpretation that state law defines a public record by its content not its context nor where it is created and stored. For purposes of public disclosure, it is not enough that communication occurs on a government issued phone, computer or device — it also has to be a communication about government business.

However, public employees' non-work-related e-mails and text messages transmitted on government provided equipment may be subject to their employer's review. The Supreme Court in *Ontario v. Quon* (*see* Federal Case Law, Section 2.0) determined that a governmental employer had a legitimate interest in reviewing the text messages that an employee sent during working hours from his employer-provided pager, and that the employer's review of such messages did not violate the employee's Fourth Amendment rights. The Court noted that if a search is conducted for "noninvestigatory, work-related purposes" or for "investigations of work-related misconduct," it may be reasonable if it is "justified at its inception," and if the measures used are "reasonably related to the objectives of the search" and are not "excessively intrusive."

In contrast to *Canterbury, Quon* holds that, while assuming employees may have an expectation of privacy in their communications sent on government-owned devices, the government employer may review the messages if the employee has knowledge of the organization's policy [of its right to review all workplace communications], the review is motivated by a legitimate work-related purpose and the review is not excessive in scope. A government employer's review of its employees' text messages for a legitimate, work-related purpose is not the same as a FOIA request to access an employee's personal communications that are not related to the public's business.

6.0. Payment Card Industry Data Security Standards (PCIDSS)

Description:

These industry standards are not law, but have been developed by credit card companies to create a single set of requirements for consumer data protection. The PCIDSS also specifically identify that credit card companies should protect stored data, encrypt transmission of cardholder data and sensitive information across public networks, and maintain a policy that addresses information security. PCIDSS applies to all members of the PCI Security Standards Council, merchants, and service providers that store, process or transmit cardholder data. Additionally, these security requirements apply to all "system components" which are defined as any network component, server, or application included in, or connected to, the cardholder data environment. Network components, include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP. Applications include all purchased and custom applications, including internal and external (web) applications.

In October, 2010 the Security Standards Council published two whitepapers concerning PCIDSS. The first titled "PCIDSS Applicability in an EMV Environment," discussed PCIDSS in the wider framework of the global standard established by Europay, Mastercard, and Visa which use integrated circuit cards (aka smart cards) to enhance security. However, while EMV stands to improve security no action is required from the State as the EMV environment today does not in all cases fulfill PCIDSS requirements or protect cardholder confidentiality and sensitive authentication data. The second white paper, "Initial Roadmap: Point-to-Point Encryption Technology and PCIDSS Compliance" covered P2PE (point-to-point encryption) as a means to simplify PCIDSS compliance standards. It found that implementation of P2PE was "immature" and that standardization would be needed before consistent security practices could be realized. In March, 2011, the Security Standards Council issued an information supplement titled "Protecting Telephone-based Payment Card Data" (the "Supplement"); it does not replace or supersede any PCIDSS requirements but is only intended to provide supplemental guidance. The Supplement provides information and guidance for merchants and service providers (i.e. call centers) who accept and/or process payment card data over the telephone; specifically clarifying the requirements as to voice recordings and what Sensitive Authentication Data may be maintained and what should be destroyed. Then in September 2011, the Security Standards Council issued the Report on Compliance (ROC) as guidance to assessors to ensure that proper and consistent level of reporting is maintained.

Source:

https://www.pcisecuritystandards.org/

Best Practices:

- Build and maintain secure computer networks and applications.
- Protect cardholder data.

- Limit access.
- Respond quickly and efficiently to incidents.
- Be aware and protect against the latest threats regarding credit card use and stored data.
- If payments are received by phone and if those calls are recorded, then technology should be used to delete or prevent the recordation or the recovery of Sensitive Authentication Data from those recordings.

Principles:
Security Safeguards, Accountability, Minimum Necessary and Limited Use